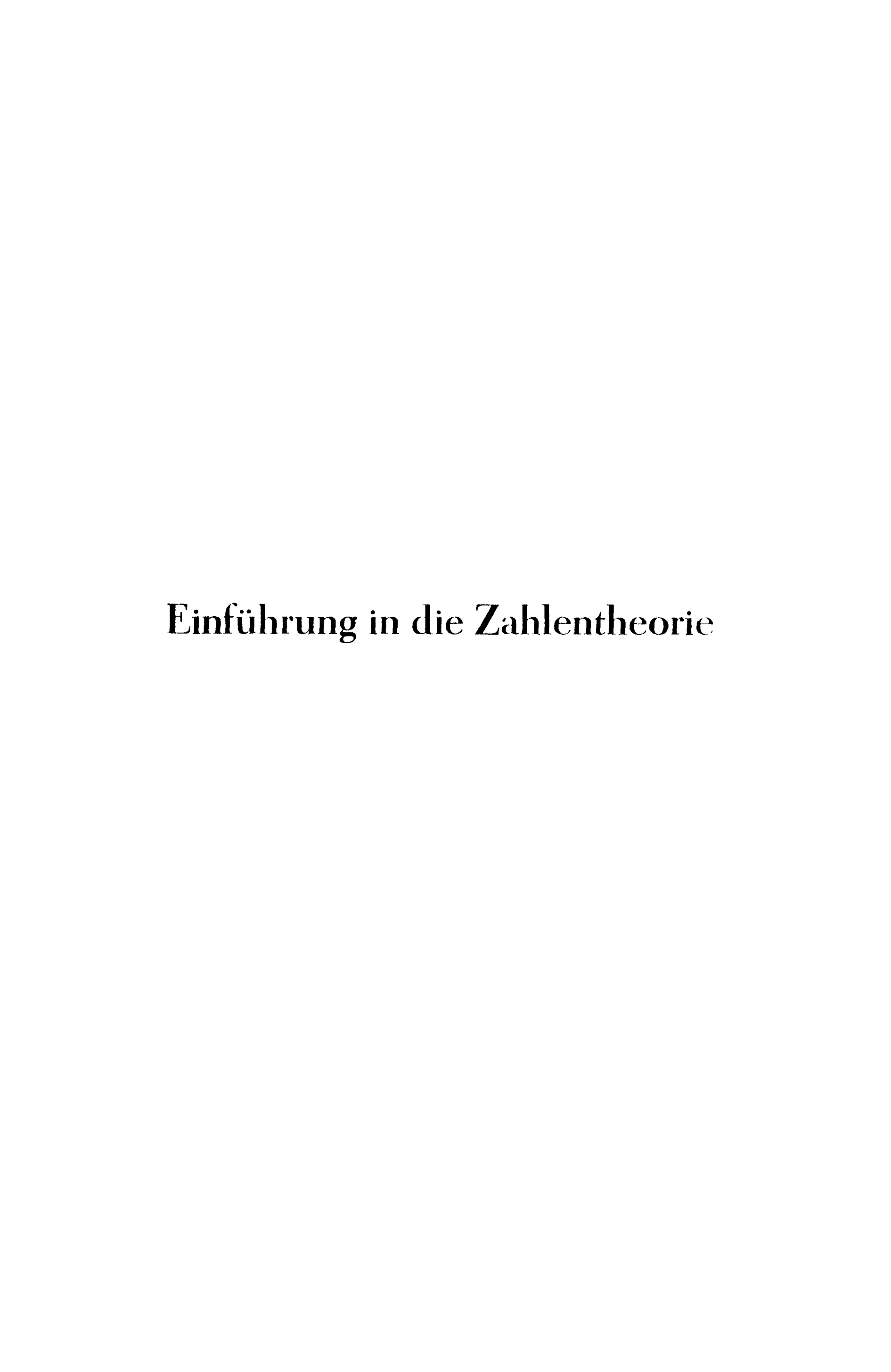
THE BOOK WAS DRENCHED

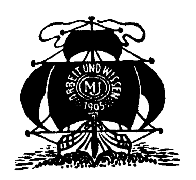


Einführung in die Zahlentheorie

Einführung in die Zahlentheorie

Von

Heinrich W. E. Jung
o. ö. Professor an der Martin Luther-Universität
Halle-Wittenberg



1935

Dr. Max Jänecke, Verlagsbuchhandlung in Leipzig



Piererscche Hofbuchdruckerei Stephan Geibel & Co., Altenburg (Thür.)

Vorrede.

Die einfachsten Gesetzmäßigkeiten, die für die ganzen Zahlen gelten, sind so auffällig, daß sie bei nur geringer Anleitung wohl jeder finden kann. Eine solche Anleitung soll die folgende Einführung in die Zahlentheorie sein. Der Leser muß sich zum Beispiel redlich bemühen, die Eigentümlichkeiten von nach gegebener Vorschrift hergestellten Tabellen selbst herauszufinden, vielleicht auch zu beweisen, ehe er weiterliest und nachsieht, welches diese Eigentümlichkeiten sind. Er wird dann die Sätze der elementaren Zahlentheorie nicht nur kennen lernen, sondern mit ihnen vertraut werden. So hoffe ich wenigstens. In dieser Hinsicht wird das Buch auch den Studierenden zur Vertiefung des Verständnisses der Vorlesung von Nutzen sein.

Zum Verständnis des Buches ist an Vorkenntnissen nur Vertrautheit mit den vier Grundrechenarten für positive und negative Zahlen nötig, so daß das Buch auch von Schülern der oberen Klassen höherer Lehranstalten verstanden werden kann und auch zum Gebrauch bei Arbeitsgemeinschaften geeignet ist.

Für die Durchsicht des Manuskripts und Ratschläge bei seiner Abfassung bin ich Frl. Studienassessorin E. Görig, Frl. Dr. M. Oehlert und besonders Herrn Dipl.-Ing. W. Leidheuser zu großem Danke verpflichtet. Weiteren Dank schulde ich dem Herrn Verleger, der auf meine Anregungen und Wünsche stets bereitwillig eingegangen ist und die Herausgabe des Buches ermöglicht hat.

Halle-S., Dezember 1934. Der Verfasser.

Inhaltsverzeichnis.

Seite

Vorrede V

I. Von den Teilern und Vielfachen der Zahlen 1
1. Teiler und Vielfache 1
2. Primzahlen und zusammengesetzte Zahlen 2
3. Gemeinsame Teiler und größter gemeinsamer Teiler . . 2
4. Teilerfremde Zahlen 4
5. Gemeinschaftliche Vielfache und das kleinste gemeinschaftliche Vielfache 5
6. Sätze über Primzahlen 6

II. Rechnen nach einem Modul 8
1. Restsysteme 8
2. Rest, den Summe, Differenz und Produkt zweier Zahlen bei der Teilung durch eine andere lassen 9
3. Rechnen nach einem Modul 10
4. Einige Beispiele 11

III. Teilbarkeitsregeln 11
1. Teilbarkeit durch 2, 4, 8 11
2. Teilbarkeit durch 5, 25, 125 12
3. Teilbarkeit durch 3, 9 12
4. Teilbarkeit durch 11 13
5. Neuner- und Elferprobe 13

IV. Multiplikationstabellen 14
1. Additionstabellen 14
2. Multiplikationstabellen 15
3. Tabellen 16
4. Eigenschaften der Tabellen 18
5. Division 19
6. Diophantische Gleichungen 23
7. Einige Bemerkungen über Divisionsaufgaben nach einem Modul 24
8. Division einer Gleichung nach einem Modul durch eine Zahl 25

V. Die Funktion $\varphi(n)$ 26
1. Die Definition 26
2. Bestimmung von $\varphi(n)$, wenn n die Potenz einer Primzahl ist 27
3. Ein Satz über $\varphi(n)$ 27
4. Eine Formel für $\varphi(n)$ bei beliebigem n 31
5. Eine Anwendung der Tabellen in Nr. 3 32

Seite

6. Eine Aufgabe 33
7. Bemerkung zur Division nach einem Modul 35
8. Noch ein Satz über $\varphi(n)$ 36

VI. Der kleine Fermatsche Satz 37
1. Die Potenzen einer Primzahl nach einer Primzahl als Modul 37
2. Der kleine Fermatsche Satz 39
3. Eine Verallgemeinerung 40
4. Eine weitere Verallgemeinerung 41
5. Über die Zahl λ 44
6. Der Fall $a = 2$ 47

VII. Quadratische Reste 49
1. Definition 49
2. Anzahl der QR und QN einer Primzahl 50
3. Produkte von QR und QN 51
4. Das Legendresche Symbol 52
5. Eine Formel für (a/p) 54
6. Der Fall $a = -1$ 57
7. Der Fall $a = 2$ 57
8. Das quadratische Reziprozitätsgesetz 57
9. Beweis des Reziprozitätsgesetzes 59
10. Berechnung von (a/p) 63
11. Vereinfachung der Rechnung durch das Jacobische Symbol 66
12. Zwei Aufgaben 70
13. Quadratische Reste von der Potenz einer ungeraden Primzahl 70
14. Quadratische Reste einer Potenz von 2 73
15. Quadratische Reste von einer ganzen Zahl m 75
16. Die Wurzel aus a nach einem Modul m 80
17. Ein Beispiel 81
18. Eine Verallgemeinerung des Wilsonschen Satzes 83

VIII. Logarithmen 85
1. Potenztabellen 85
2. Eigenschaften der PT 86
3. Beweis der Eigenschaften der PT 88
4. Logarithmen 91
5. Eigenschaften der Logarithmen 94
6. Anwendungen 95
7. Wurzeln. Potenzreste 98
8. Über die Verallgemeinerung des Logarithmus 101
Sachregister 105

I. Von den Teilern und Vielfachen der Zahlen.

Unter einer Zahl ist immer eine ganze Zahl zu verstehen.

1. Teiler und Vielfache.

Ziehen wir von 38 wiederholt 7 ab, so erhalten wir der Reihe nach die Zahlen 31, 24, 17, 10, 3. Wir können also 7 fünfmal von 38 subtrahieren, bis wir zu einer Zahl kommen, die kleiner ist als 7. Daher ist

$$38 = 5 \cdot 7 + 3.$$

Wir sagen: 7 ist fünfmal in 38 enthalten, und der *Rest* ist 3. Oder, wenn wir von 52 die Zahl 13 wiederholt abziehen, so erhalten wir die Zahlen 39, 26, 13, 0, so daß wir 13 von 52 viermal subtrahieren können, und der Rest ist 0. Daher ist

$$52 = 4 \cdot 13 + 0.$$

Allgemein seien a und m zwei positive ganze Zahlen. Ist $a > m$ (die Zeichen $>$ und $<$ bedeuten „größer als" und „kleiner als"), so können wir m von a abziehen, und wenn die Differenz $a - m \geq m$, so können wir m nochmal abziehen, und das können wir so lange fortsetzen, bis wir entweder 0 oder eine positive Zahl erhalten, die kleiner ist als m. Haben wir m q-mal von a subtrahiert, so ist

(1) $$a = qm + r, \text{ wo } 0 \leq r < m.$$

Wir sagen: m ist q-mal in a enthalten, und der Rest ist r. Die Darstellung (1) von a gilt auch, wenn $a < m$; es ist dann $q = 0$, $a = r$. Aber es kann a auch negativ sein. Wir haben dann m so oft zu a zu addieren, bis wir 0 oder eine positive Zahl r erhalten, die kleiner ist als m. So ist $-35 + 3 \cdot 13 = 4$ oder $-35 = (-3) \cdot 13 + 4$. Die durch (1) ausgedrückte Tatsache, daß man aus einer Zahl a durch Subtraktion eines passenden Vielfachen, etwa des q-fachen, einer anderen Zahl m, eine Zahl r, den Rest, erhalten kann, die der Bedingung $0 \leq r < m$ genügt, ist für das Folgende sehr wichtig. Die Zahl q kann dabei auch 0 oder negativ sein.

Uns interessiert zunächst nur der Fall, wo der Rest r gleich 0 ist, wo also

(2) $$a = qm.$$

Wir sagen in diesem Fall: a ist durch m teilbar, m teilt a, m ist in a enthalten, m ist *Teiler* von a oder a ist *Vielfaches* von m. Das soll auch dann gelten, wenn $q = 1$, also $a = m$, und wenn $q = a$, also $m = 1$. Zum Bei-

spiel hat 35 die Teiler 1, 5, 7, 35, und es ist 35 ein Vielfaches von 1, 5, 7 und auch von 35, wenn es auch nur das Einfache von 35 ist. Es darf aber q auch gleich 0 sein. Dann ist natürlich auch $a = 0$, während m ganz beliebig gewählt werden kann. Hiernach ist 0 Vielfaches jeder Zahl, und jede Zahl ist Teiler von 0.

Wir wollen im folgenden die Teiler immer als positive Zahlen wählen.

2. Primzahlen und zusammengetzte Zahlen.

Wir betrachten in dieser Nummer nur positive Zahlen.

Es gibt eine Zahl mit nur einem Teiler, nämlich 1.

Es gibt Zahlen mit genau zwei Teilern, z. B. 2, 3, 5, 7, 11, 13. Diese haben nur 1 und sich selbst als Teiler. Sie heißen *Primzahlen.*

Es gibt eine Zahl mit unendlich vielen Teilern, nämlich 0, wie wir schon in der vorigen Nummer gesehen haben.

Alle anderen ganzen Zahlen heißen *zusammengesetzte Zahlen.* Jede solche Zahl m läßt sich mindestens auf eine Art als Produkt $l \cdot n$ darstellen, wo die beiden Faktoren l und n beide von 1 und von m verschieden sind. Es hat daher eine zusammengesetzte Zahl m außer den selbstverständlichen Teilern 1 und m mindestens noch einen anderen, der größer als 1 und kleiner als m ist. Derartige Teiler heißen *echte* oder *eigentliche Teiler.*

3. Gemeinsamer Teiler (g. T.) und größter gemeinsamer Teiler (g. g. T.) gegebener Zahlen.

Die Zahlen 15, 20, 225 haben alle drei den Teiler 5. Man nennt 5 einen *gemeinsamen Teiler* (g. T.) dieser Zahlen. Die Zahlen 140, 210, 490 haben die gemeinsamen Teiler 1, 2, 5, 7, 10, 14, 35, 70. Ihr *größter gemeinsamer Teiler* (g. g. T.) ist 70. Er ist durch alle anderen teilbar. Die Zahlen 84, 420, 294 haben die g. T. 1, 2, 3, 6, 7, 14, 21, 42. Der größte, 42, ist wieder durch die anderen teilbar.

Es ergibt sich die Aufgabe, die g. T. und vor allem den g. g. T. gegebener Zahlen zu bestimmen. Zunächst: Haben zwei Zahlen a, b den g. T. h, sind also beide Vielfache von h, so gilt dasselbe von ihrer Summe und Differenz. Ist etwa a das 3-fache und b das 7-fache von h, so ist die Summe das 10-fache und die Differenz das (—4)-fache von h. Sind also irgendwelche Zahlen, z. B. a, b, c, gegeben, die h als g. T. haben, so haben auch alle Zahlen, die aus a, b, c durch wiederholte Addition und Subtraktion hervorgehen, diesen Teiler. Wir nennen die Gesamtheit der Zahlen, die man auf diese Art aus gegebenen Zahlen erhält, einen *Ring.* Wir bezeichnen den aus den Zahlen a, b, c entstehenden Ring mit $\{a, b, c\}$. Alle

Zahlen dieses Ringes sind also durch h teilbar, vor allem auch die kleinste positive Zahl, die in dem Ring enthalten ist. Ehe wir weitergehen, bestimme man in den folgenden Ringen die kleinste positive Zahl.

1. $\{6, 12, 22\}$, 2. $\{6, 15, 22\}$, 3. $\{130, 5250\}$, 4. $\{6655, 215610\}$.

Es sind die Zahlen 2, 1, 10, 5. Um sie zu finden, kann man systematisch so verfahren: Zunächst ist mit a nach Definition auch $a - a = 0$ und dann auch $0 - a = -a$ im Ringe enthalten. Zwei sich nur durch das Vorzeichen unterscheidende Zahlen sind daher immer beide im Ring enthalten oder beide nicht. Wir können und wollen uns daher auf die positiven Zahlen beschränken und nehmen auch die gegebenen Zahlen positiv an. Man ziehe die kleinste der gegebenen Zahlen, es sei a, von den anderen so oft ab, bis man 0 oder positive Zahlen erhält, die kleiner sind als a. Dann subtrahiere man die kleinste der so erhaltenen Zahlen so oft von den anderen, bis man wieder kleinere Zahlen bekommt, und so fährt man fort. Da man auf diese Art immer kleinere positive Zahlen erhält, so muß man schließlich zu einer kleinsten kommen. Diese sei d. Subtrahieren wir dann d wiederholt von irgendeiner Zahl des Ringes, so dürfen wir keine positive Zahl erhalten, die kleiner ist als d; es muß sich also der Rest 0 ergeben. Das heißt aber, jede Zahl des Ringes, im besonderen also auch jede der gegebenen Zahlen, ist durch d teilbar. Andererseits sind mit d auch $d + d = 2d$, $2d + d = 3d$, $3d + d = 4d, \ldots$ im Ringe enthalten, d. h. alle Vielfachen von d. Der Ring besteht daher aus der Zahl 0 und aus allen positiven und negativen Vielfachen von d. Dabei ist d die kleinste positive Zahl, die in dem Ringe enthalten ist.

Der Ring sei etwa durch drei Zahlen a, b, c gegeben. Wir sind davon ausgegangen, daß jeder g. T. von a, b, c in jeder Zahl des Ringes $\{a, b, c\}$ aufgeht. Er ist also auch in d enthalten. Da aber a, b, c durch d teilbar sind, so folgt einmal:

Die kleinste in einem Ringe $\{a, b, c\}$ enthaltene positive Zahl ist der g. g. T. von a, b, c.

Und dann: *Jeder g. T. irgendwelcher Zahlen ist in ihrem g. g. T. enthalten, und jeder Teiler des g. g. T. ist g. T.*

Wir bezeichnen den g. g. T. zweier Zahlen a, b mit (a, b), den g. g. T. dreier Zahlen a, b, c mit (a, b, c) usw.

Zur praktischen Berechnung der kleinsten positiven Zahl, die in einem Ring enthalten ist, sei noch folgendes gesagt. Man wird im Beispiel 3 die Zahl 130 nicht 40mal einzeln von 5250 abziehen, sondern gleich das 40-fache von 130, also 5200, und erhält so die neue dem Ringe angehörende Zahl 50. Ebenso wird man im Beispiel 4 die größere Zahl durch die kleinere dividieren, um zu sehen, wie oft man diese von jener abziehen kann, ohne daß die Differenz negativ wird. Man findet als Ergebnis der Division 32

und den Rest 2650. Diesen erhält man aus der Zahl 215610 durch Subtraktion des 32fachen von 6655. Es gehört also der Rest 2650 auch dem Ringe an.

Aufgabe: Zu beweisen: 1. Jede Zahl des Ringes $\{a, b\}$ läßt sich in der Form $ax + by$ darstellen, wo x und y ganze, nicht notwendig positive Zahlen sind. Ebenso kann man jede Zahl aus $\{a, b, c\}$ in der Form $ax + by + cz$ darstellen, wo x, y, z ganze Zahlen sind.

2. Es ist

$$(a, b) = (a + b, a) = (a + b, b) = (a - b, a) = (a - b, b).$$

Frage: Wie müssen a und b beschaffen sein, damit

$$(a, b) = (a + b, a - b)?$$

4. Teilerfremde Zahlen.

Zahlen, die den g. g. T. 1 haben, heißen teilerfremd. Bei mehr als zwei Zahlen muß man wohl unterscheiden zwischen teilerfremd und *zu je zweien teilerfremd.* So sind z. B. 6, 10, 15 teilerfremd, aber nicht zu je zweien teilerfremd. Natürlich sind Zahlen, die zu je zweien teilerfremd sind, auch im ganzen teilerfremd. Es ist ja der g. g. T. von irgendwelchen Zahlen schon dann 1, wenn auch nur zwei von ihnen teilerfremd sind. Aber es gilt nicht das Umgekehrte.

Entsprechende Zahlen des Ringes $\{a, b, c\}$ und des Ringes $\{ah, bh, ch\}$, d. h. Zahlen, die durch dieselbe Folge von Additionen und Subtraktionen aus den Anfangszahlen hervorgehen, unterscheiden sich durch den Faktor h. So entspricht der Zahl $3a - 5b + 7c$ des ersten die Zahl $3\,ah - 5\,bh + 7ch = (3a - 5b + 7c)\,h$ des zweiten Ringes. Ist also die kleinste positive Zahl im ersten Ringe d, so im zweiten dh. Oder wegen der oben gefundenen Bedeutung dieser Zahlen:

Ist $(a, b, c) = d$, so ist $(ah, bh, ch) = dh$.

Im besonderen gilt:

Ist $(a, b) = 1$, so ist $(ah, bh) = h$.

Daraus ergibt sich folgender wichtige Satz:

Ist a teilerfremd zu b, und ist a h durch b teilbar, so ist h durch b teilbar.

Es ist nämlich h der g. g. T. von $a\,h$ und $b\,h$ und nach Voraussetzung ist b g. T. von ah und bh. Da aber jeder g. T. im g. g. T. enthalten ist, so ist, wie behauptet, h durch b teilbar.

Wir betrachten noch den besonderen Fall, wo die eine Zahl, etwa b, eine Primzahl p ist. Da p nur die Teiler 1 und p hat, so ist eine Zahl a entweder teilerfremd zu p oder durch p teilbar, so daß (a, p) nur gleich 1 oder p sein kann. Es seien l, m zwei Zahlen. Ist lm durch p teilbar, so kann l durch p teilbar sein. Ist aber l nicht durch p teilbar, also teiler-

fremd zu p, so ist nach dem eben bewiesenen Satze m durch p teilbar. Es ist also ein Produkt lm von zwei Faktoren dann und nur dann durch eine Primzahl p teilbar, wenn mindestens einer der Faktoren durch p teilbar ist. Das gilt auch für Produkte von mehr Faktoren. Darauf gehen wir hier nicht ein, da wir später auf anderem Wege darauf zurückkommen.

Es gilt noch: Sind p und q zwei Primzahlen, so ist entweder $p = q$ oder $(p, q) = 1$.

5. Gemeinschaftliche Vielfache (g. V.) und das kleinste gemeinschaftliche Vielfache (k. g. V.) gegebener Zahlen.

Eine *von 0 verschiedene* Zahl, die durch jede einzelne von gegebenen Zahlen teilbar ist, die also Vielfaches einer jeden ist, heißt *gemeinschaftliches Vielfaches* (g. V.) von ihnen. Ein solches ist zum Beispiel ihr Produkt. Das *kleinste gemeinschaftliche Vielfache* (k. g. V.) zweier Zahlen a, b bezeichnen wir mit $[a, b]$, das von drei Zahlen a, b, c mit $[a, b, c]$ usw.

Wir betrachten zunächst zwei Zahlen, etwa 70 und 45. Ihr g. g. T. ist 5 und es ist $70 = 5 \cdot 14$, $45 = 5 \cdot 9$. Das Produkt der beiden Zahlen

$$70 \cdot 45 = 14 \cdot 5 \cdot 5 \cdot 9$$

ist g. V. von ihnen. Durch $14 \cdot 5$ und durch $9 \cdot 5$ teilbar ist aber schon

$$m = 14 \cdot 5 \cdot 9 = \frac{70 \cdot 45}{5} \cdot$$

Der g. g. T. ist offenbar nur einmal nötig. Ist andererseits l irgendein Vielfaches von 70 und 45, so muß l zunächst durch 70 teilbar sein, also die Form haben $70n$, wo n eine ganze Zahl ist. Ferner muß $l = 70n = 14 \cdot 5 \cdot n$ durch $45 = 9 \cdot 5$ teilbar sein, also $14n$ durch 9. Da aber 14 teilerfremd zu 9 ist, so muß n 9 enthalten, also von der Form $9g$ sein. Es wird somit

$$l = 70n = 70 \cdot 9 \cdot g = \frac{70 \cdot 45}{5} g = mg.$$

Daher ist jedes g. V. von 70 und 45 Vielfaches von m. Und m ist das k. g. V. von 70 und 45. Wir haben so gefunden:

Das Produkt zweier positiver Zahlen ist gleich dem Produkt ihres g. g. T. und ihres k. g. V. ($[a, b] \cdot (a, b) = a \cdot b$).

Jedes g. V. zweier Zahlen ist durch ihr k. g. V. teilbar. Wir zeigen noch, daß der letzte Satz auch für mehr als zwei Zahlen gilt. Es seien $a, b, c, \ldots$ ganze Zahlen. Ihr k. g. V. sei m. Ferner sei l irgendein g. V. Es sind l und m und daher auch die Zahlen $l - m$, $l - 2m$, $l - 3m, \ldots$ durch jede der gegebenen Zahlen teilbar, also g. V. von ihnen. Wir können aber

die Zahl q so bestimmen, daß $l - qm$ gleich 0 oder positiv und kleiner als m ist. Würde der zweite Fall eintreten, so wäre $l - qm$ ein g. V., das kleiner wäre als m, und m wäre nicht das k. g. V. Daher ist $l - qm = 0$, $l = qm$ und l, wie behauptet, Vielfaches von m. Also:

Jedes g. V. irgendwelcher Zahlen ist durch ihr k. g. V. teilbar.

Es seien drei Zahlen gegeben, $a = 35$, $b = 21$, $c = 14$, und es sei ihr k. g. V. m zu bestimmen. Es muß m ein Vielfaches von a und b sein, also ein Vielfaches des k. g. V. von 35 und 21, d. h. von $35 \cdot 21/7 = 105$. Es ist daher m das k. g. V. von 105 und 14, so daß

$$[35,\ 21,\ 14] = [105,\ 14] = \frac{105 \cdot 14}{7} = 210.$$

Aufgabe. Zu beweisen: Das k. g. V. von zu je zweien teilerfremden Zahlen ist ihr Produkt.

6. Sätze über Primzahlen.

Wir wiederholen zunächst:

Eine Zahl, die genau zwei Teiler hat, ist eine Primzahl.

Es ist also 1 keine Primzahl. Es gibt eine gerade Primzahl, nämlich 2; alle anderen sind ungerade. Ferner:

Sind p und q Primzahlen, so ist entweder $p = q$ oder $(p, q) = 1$.

Ist von zwei Primzahlen die eine durch die andere teilbar, so sind sie einander gleich.

Wir können jetzt den Satz beweisen:

Jede Zahl, außer 1, ist entweder Primzahl oder sie läßt sich auf eine und nur auf eine Art als Produkt von Primzahlen darstellen.

So ist z. B. $60 = 2 \cdot 2 \cdot 3 \cdot 5$, $1001 = 7 \cdot 11 \cdot 13$, $2001 = 3 \cdot 23 \cdot 29$, $1024 = 2^{10}$. Der erste Teil unseres Satzes, daß sich nämlich jede Zahl als Produkt von Primzahlen darstellen läßt, wenn sie nicht 1 oder selbst eine Primzahl ist, ergibt sich so: Es sei a eine Zahl größer als 1. Ist sie nicht selbst Primzahl, so läßt sie sich als Produkt gh darstellen, wo g und h echte Teiler von a sind, also kleiner als a und nicht gleich 1. Sind g und h beides Primzahlen, so ist a in der behaupteten Art zerlegt. Ist aber etwa g keine Primzahl, so läßt sich g als Produkt lm darstellen, wo l und m nicht gleich 1 und kleiner als g sind. Es wird $a = lmh$. Sind l, m, h Primzahlen, so ist a in gewünschter Weise zerlegt. Im andern Falle läßt sich mindestens einer der Faktoren l, m, h weiter in echte Teiler zerlegen. So können wir fortfahren und müssen schließlich zu Faktoren kommen, die sich nicht weiter zerlegen lassen, also zu Primzahlen, da bei jedem Schritt die Faktoren kleiner werden. Es gibt nicht immer nur einen Weg, der auf die angegebene Art zur vollständigen Zerlegung von a führt. Es sei z. B.

$a = 30030$. Wir können a beim ersten Schritt zerlegen in $30 \cdot 1001$ oder in $70 \cdot 429$, $154 \cdot 195$ usw. Es ist nicht selbstverständlich, daß die weitere Zerlegung immer zum selben Endergebnis führt. Wir müssen daher noch zeigen, daß die Zerlegung nur auf eine Art möglich ist. Wir beweisen, daß die Annahme des Gegenteils auf einen Widerspruch führt. Es gebe also Zahlen, die sich auf mehr als eine Art als Produkt von Primzahlen darstellen lassen. Es sei a die kleinste von ihnen. Zwei verschiedene Zerlegungen von a seien

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n. \tag{3}$$

Die Primzahlen p_i sind alle von den q_k verschieden. Wäre z. B. $p_2 = q_3$, so könnten wir die Gleichung (3) mit p_2 dividieren, und wir würden eine Zahl, nämlich a/p_2 erhalten, die kleiner ist als a, und die sich auch auf verschiedene Arten zerlegen läßt. Zur Abkürzung sei $q_2 q_3 \cdots q_n = b$ gesetzt, so daß $a = q_1 b$. Aus (3) folgt, daß $q_1 b$ durch p_1 teilbar ist. Da q_1 von p_1 verschieden und daher teilerfremd zu p_1 ist, so muß b durch p_1 teilbar sein. Es sei $b = p_1 c$. Aus (3) folgt durch Division mit p_1

$$a' = a/p_1 = p_2 p_3 \cdots p_m = q_1 c.$$

Zerlegen wir hierin c auf irgendeine Art in Primfaktoren, so erhalten wir für a' zwei Zerlegungen, die sicher voneinander verschieden sind. Denn die zweite enthält die Primzahl q_1, die in der ersten nicht vorkommt. Da aber a' kleiner ist als a, so haben wir einen Widerspruch.

Wir zeigen noch, daß es unendlich viele Primzahlen gibt. Es gebe nämlich nur eine endliche Anzahl, etwa n. Diese n Primzahlen seien $p_1, p_2, \ldots, p_n$. Die Zahl

$$a = p_1 p_2 \cdots p_n + 1 \tag{4}$$

ist durch keine der Zahlen p_k teilbar, da sie bei der Teilung durch jede von ihnen den Rest 1 läßt. Sie ist aber entweder Primzahl oder ist durch Primzahlen teilbar, und diese sind von den Zahlen p_k sicher verschieden, da sie Teiler von a sind. Es muß daher außer den n Primzahlen p_k noch andere geben.

Aus dem Beweise ergibt sich, daß die Zahl a in (4), wo die p_k irgendwelche Primzahlen sind, nur Primzahlen als Teiler enthält, die von den p_k verschieden sind. Z. B.:

$$2 \cdot 5 + 1 = 11, \quad 3 \cdot 5 + 1 = 2^4, \quad 2 \cdot 7 \cdot 11 + 1 = 155 = 5 \cdot 31,$$
$$3 \cdot 23 \cdot 29 + 1 = 2002 = 2 \cdot 7 \cdot 11 \cdot 13.$$

Aufgabe: Man bestimme den g. g. T. und das k. g. V. gegebener Zahlen, indem man ihre Zerlegungen in Produkte von Primzahlen benutzt.

II. Rechnen nach einem Modul.

1. Restsysteme.

Wie wir in I, 1 gesehen haben, läßt sich, wenn m irgendeine Zahl ist, jede Zahl a in der Form darstellen.

(5) $$a = qm + r, \text{ wo } 0 \leqq r < m.$$

Mit anderen Worten: Wir können von jeder Zahl a ein solches Vielfaches von m — unter Umständen ein negatives — abziehen, daß als Rest eine der Zahlen

(6) $$0, 1, 2, \ldots, m-1$$

bleibt. Es sei etwa $m = 7$. Dann sind die möglichen Reste

(7) $$0, 1, 2, 3, 4, 5, 6.$$

Ist der Rest eine der Zahlen 4, 5, 6, und subtrahiert man dann noch einmal 7, so erhält man die Reste —3, —2, —1. Zum Beispiel ist

$$75 = 10 \cdot 7 + 5 = 11 \cdot 7 - 2, \quad -22 = -4 \cdot 7 + 6 = -3 \cdot 7 - 1.$$

Wir können daher auch jede Zahl a so in der Form

(8) $$a = q \cdot 7 + r$$

darstellen, daß der Rest r eine der Zahlen

(9) $$-3, -2, -1, 0, 1, 2, 3$$

ist. Allgemein können wir, wenn m eine ungerade Zahl ist, jede Zahl a so in der Form (5) darstellen, daß der Rest r eine der Zahlen

(10) $$0, \pm 1, \pm 2, \ldots, \pm \frac{1}{2}(m-1)$$

ist. Man nennt die Reste (6) und (7) die *positiv kleinsten Reste* und die Reste (9) und (10) die *absolut kleinsten Reste.* Wenn nichts anderes gesagt ist, wählen wir im folgenden immer die positiv kleinsten Reste.

Aufgabe. Zu zeigen: Addiert man zu jeder der Zahlen (7) irgendein Vielfaches von 7, nicht notwendig zu jeder dasselbe, so erhält man sieben Zahlen

(11) $$r_1, r_2, \ldots, r_7,$$

so daß man jede Zahl a so in der Form (8) darstellen kann, daß jetzt r eine der Zahlen (11) ist.

Man nennt sieben derartige Zahlen ein *vollständiges* oder *volles Restsystem* von 7. Ein solches ist z. B.:

$$14, -6, -12, 73, 4, 40, -1.$$

Jede Zahl geht aus einer und nur aus einer der Zahlen eines vollen Restsystems durch Hinzufügen eines positiven oder negativen Vielfachen von 7 hervor, oder sie ist selbst eine dieser Zahlen. Daraus folgt, daß zwei

Zahlen, die denselben Rest eines bestimmten Restsystems bei der Teilung durch 7 lassen, sich nur durch ein Vielfaches von 7 unterscheiden, daß sie das aber nicht tun, wenn sie verschiedene Reste lassen. Oder gleich allgemein:

Zwei Zahlen g und h lassen dann und nur dann bei der Teilung durch eine Zahl m denselben Rest eines bestimmten, fest gewählten Restsystems, wenn ihre Differenz $g - h$ durch m teilbar ist.

2. Rest, den Summe, Differenz und Produkt zweier Zahlen bei der Teilung durch eine andere lassen.

Es seien g und h zwei Zahlen, und es sei m eine positive Zahl. Es mögen g und h bei der Teilung durch m die Reste r und s lassen. Wir untersuchen, welchen Rest $g + h$, $g - h$, gh lassen. Es sei

$$g = km + r, \quad h = lm + s. \tag{12}$$

Zunächst seien g und h positiv und $g > h$; ferner seien r und s die positiv kleinsten Reste. Die Gleichungen (12) können wir anschaulich so deuten: Verteilen wir g (h) Nüsse gleichmäßig unter m Jungen, so erhält jeder k (l) und es bleiben r (s) übrig. Wollen wir $g + h$ Nüsse gleichmäßig unter m Jungen verteilen, so können wir erst g und dann h verteilen. Von den ersten g bleiben r und von den zweiten h bleiben s übrig, im ganzen also $r + s$. Ist $r + s \geqq m$, so kann man noch weiter verteilen. Auf jeden Fall ist der bei der Verteilung von $g + h$ Nüssen verbleibende Rest geradeso groß wie der bei der Verteilung von $r + s$ Nüssen. Es sei jetzt $r \geqq s$. Um zu sehen, welcher Rest bei der Verteilung von $g - h$ Nüssen bleibt, denken wir uns zunächst wieder g Nüsse verteilt, so daß r übrig bleiben; dann nehmen wir h Nüsse in der Weise fort, daß wir uns von jedem Jungen l Nüsse geben lassen, während wir den Rest von s Nüssen von dem vorher gebliebenen Rest von r Nüssen wegnehmen. Es bleiben daher $r - s$ Nüsse übrig. Es seien jetzt gh Nüsse zu verteilen. Wir denken sie uns in g Kästen, so daß in jedem h liegen. Wir können dann zunächst jedem Jungen k Kästen geben, so daß r Kästen und rh Nüsse übrig sind. Dann geben wir jedem der Jungen aus jedem der Kästen l Nüsse. Es bleiben dann in jedem der r Kästen s Nüsse, so daß der verbleibende Rest aus rs Nüssen besteht. Ist $rs \geqq m$, so kann man noch weiter verteilen; auf jeden Fall ist der bei der Verteilung von gh Nüssen verbleibende Rest gerade so groß wie der bei der Verteilung von rs.

Allgemein folgt aus (12) für beliebige Zahlen g, h und für irgendein Restsystem

$$(g + h) - (r + s) = m(k + l), \quad (g - h) - (r - s) = m(k - l),$$
$$gh - rs = m(klm + ks + lr).$$

Es sind daher die Differenzen von $g+h$ und $r+s$, von $g-h$ und $r-s$, von gh und rs durch m teilbar. Das aber bedeutet:

Lassen die Zahlen g und h bei der Teilung durch m die Reste r und s, so lassen die Zahlen $g+h$, $g-h$, gh dieselben Reste wie $r+s$, $r-s$, rs.

Wollen wir z. B. den Rest bestimmen, den

$$a = 123 \cdot 733 + 15 \cdot 79$$

bei der Teilung durch 7 läßt, so brauchen wir a keineswegs auszurechnen, sondern wir können die Zahlen 123, 733, 15, 79 durch ihre Reste 4, 5, 1, 2 ersetzen. Es läßt also

$$b = 4 \cdot 5 + 1 \cdot 2 = 22$$

denselben Rest, so daß a den Rest 1 ergibt. Oder, indem wir unseren Satz wiederholt anwenden: Es läßt bei der Teilung durch 13

$$a = 5203 \cdot 2734 \cdot 98 - 15 \cdot 130 \cdot 511 + 66 \cdot 7 \cdot 9144 \cdot 28$$

denselben Rest wie

$$b = 3 \cdot 4 \cdot 7 - 15 \cdot 0 \cdot 511 + 1 \cdot 7 \cdot 5 \cdot 2 = 84 + 70 = 154,$$

also den Rest 11. Oder es läßt 123^6 bei der Teilung durch 7 denselben Rest wie $4^6 = 4^3 \cdot 4^3 = 64 \cdot 64$ oder wie $1 \cdot 1 = 1$. Oder: Bei der Teilung durch 11 läßt $3^3 = 27$ den Rest 5; $3^4 = 3 \cdot 3^3$ läßt denselben Rest wie $3 \cdot 5 = 15$, also den Rest 4; $3^5 = 3 \cdot 3^4$ läßt denselben Rest wie $3 \cdot 4 = 12$, also den Rest 1 usw.

3. Rechnen nach einem Modul.

Wir wollen eine positive Zahl auszeichnen, etwa 5, und festsetzen, daß zwei Zahlen als gleich gelten sollen, wenn sie sich nur durch ein Vielfaches von 5 unterscheiden. Mit anderen Worten: Wir setzen fest, es soll

$$5 = 0$$

sein. Es ist dann z. B. $38 = 3 + 7 \cdot 5 = 3 + 7 \cdot 0 = 3$, $-21 = -1 = 4 = 24$ usw. Es ist jede Zahl gleich einer der fünf Zahlen

$$0,\ 1,\ 2,\ 3,\ 4 \tag{13}$$

oder auch gleich einer der Zahlen

$$-2,\ -1,\ 0,\ 1,\ 2. \tag{14}$$

Wir können uns also auf die Zahlen (13) oder (14) beschränken. Wenn nichts anderes gesagt ist, benutzen wir die Zahlen (13), d. h. die positiv kleinsten Reste von 5. Das Rechnen wird dann sehr einfach, da wir überhaupt nur fünf Zahlen haben. Es ist z. B.

$$1 + 4 = 0,\ 3 - 4 = -1 = 4,\ 4 + 4 = 3,\ 2 \cdot 3 = 1,\ 3 \cdot 4 = 2,\ 4 \cdot 4 = 1.$$

Die ausgezeichnete Zahl 5 nennen wir den *Modul*, und wir sagen, wir *rechnen nach dem Modul 5* oder auch kürzer: nach 5.

Allgemeiner können wir irgendeine positive Zahl m als Modul wählen, also festsetzen, daß zwei Zahlen als gleich gelten sollen, wenn sie sich durch ein Vielfaches von m unterscheiden. Es ist dann z. B. $m = 0$, $3m + 5 = 5$, $m^2 = m^3 = 0$ usw. Den in der vorigen Nummer bewiesenen Satz können wir jetzt so aussprechen:

Ist $g = r$, $h = s$ *nach dem Modul* m, *so ist auch* $g + h = r + s$, $g - h = r - s$, $gh = rs$ *nach dem Modul* m.

Im besonderen folgt aus $g = r$ auch $g^2 = r^2$, $g^3 = r^3$ usw. nach m.

Da jede Zahl sich von den Zahlen

$$0,\ 1,\ 2, \ldots, m - 1 \tag{15}$$

nur durch ein Vielfaches von m unterscheidet, so können wir uns auf diese m Zahlen beschränken, wenn wir nach dem Modul m rechnen. Diese sind nach m voneinander verschieden. Wir können uns ebenso auf die absolut kleinsten Reste beschränken, also auf die Zahlen (10), wenn m ungerade ist.

4. Einige Beispiele.

Nach dem Modul 7 ist

$$86 = 2,\ 738 = 3,\ 9150 = 1, \text{ also } 86 \cdot 738 \cdot 9150 = 2 \cdot 3 \cdot 1 = 6.$$

Nach dem Modul 13 ist

$$67 \cdot 270 \cdot 35 - 172 \cdot 400 + 518 \cdot 40 = 2 \cdot 10 \cdot 9 - 3 \cdot 10 + 11 \cdot 1$$
$$180 - 30 + 11 = 11 - 4 + 11 = 18 = 5$$

und

$$3 + 12 \cdot 40 + 8 \cdot 40^2 + 5 \cdot 40^3 = 3 + 12 + 8 + 5 = 28 = 2.$$

Der Leser rechne noch viele, viele Beispiele.

III. Teilbarkeitsregeln.

1. Teilbarkeit durch 2, 4, 8.

Wählen wir als Modul 2, setzen wir also $2 = 0$, so wird auch $10 = 0$ und daher

$$2431 = 243 \cdot 10 + 1 = 1,\ 78253 = 7825 \cdot 10 + 3 = 3,$$

woraus folgt:

Eine Zahl läßt bei der Teilung durch 2 denselben Rest wie ihre letzte Ziffer, ist also durch 2 dann und nur dann teilbar, wenn ihre letzte Ziffer durch 2 teilbar ist.

Nach dem Modul 4 ist $100 = 0$, daher ist

$$4836 = 36 + 48 \cdot 100 = 36,\ 27485 = 85 + 274 \cdot 100 = 85$$

oder: Eine Zahl läßt bei der Teilung durch 4 denselben Rest wie die aus ihren beiden letzten Ziffern bestehende Zahl; sie ist also dann und nur dann durch 4 teilbar, wenn die aus ihren beiden letzten Ziffern bestehende Zahl durch 4 teilbar ist. Ähnlich ergibt sich:

Eine Zahl läßt bei der Teilung durch 8 denselben Rest wie die aus ihren drei letzten Ziffern bestehende Zahl; sie ist also dann und nur dann durch 8 teilbar, wenn die aus ihren letzten drei Ziffern bestehende Zahl durch 8 teilbar ist.

2. Teilbarkeit durch 5, 25, 125.

Nach dem Modul 5 ist $10 = 0$, also

$$75312 = 7531 \cdot 10 + 2 = 2, \quad 6893 = 689 \cdot 10 + 3 = 3.$$

Nach dem Modul 25 ist $100 = 0$, so daß

$$75312 = 753 \cdot 100 + 12 = 12, \quad 6893 = 68 \cdot 100 + 93 = 93.$$

Nach dem Modul 125 ist $1000 = 0$ und daher

$$75312 = 312, \quad 6893 = 893.$$

Also:

Eine Zahl läßt bei der Teilung durch 5 denselben Rest wie ihre letzte Ziffer.

Eine Zahl läßt bei der Teilung durch 25 denselben Rest wie die aus ihren beiden letzten Ziffern bestehende Zahl.

Eine Zahl läßt bei der Teilung durch 125 denselben Rest wie die aus ihren letzten drei Ziffern bestehende Zahl.

Und im besonderen:

Eine Zahl ist durch 5 dann und nur dann teilbar, wenn ihre letzte Ziffer 0 oder 5 ist.

Eine Zahl ist durch 25 dann und nur dann teilbar, wenn ihre beiden letzten Ziffern 00, 25, 50 oder 75 sind.

Eine Zahl ist durch 125 dann und nur dann teilbar, wenn ihre drei letzten Ziffern 000, 125, 250, 375, 500, 625, 750 oder 875 sind.

3. Teilbarkeit durch 3, 9.

Nach dem Modul 3 und auch nach 9 ist $10 = 1$, und daher sind auch alle Potenzen von 10 gleich 1. Also wird

$$5432 = 5 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10 + 2 = 5 + 4 + 3 + 2,$$
$$78214 = 7 \cdot 10^4 + 8 \cdot 10^3 + 2 \cdot 10^2 + 1 \cdot 10 + 4 = 7 + 8 + 2 + 1 + 4.$$

Nennen wir die Summe der Ziffern einer Zahl ihre *Quersumme*, so haben wir:

Eine Zahl läßt bei der Teilung durch 3 oder 9 denselben Rest wie ihre Quersumme, und sie ist dann und nur dann durch 3 oder 9 teilbar, wenn ihre Quersumme es ist.

4. Teilbarkeit durch 11.

Nach dem Modul 11 ist $10 = -1$, so daß die geraden Potenzen von 10 gleich $+1$ und die ungeraden gleich -1 sind. Daher ist

$$3475 = 5 + 7 \cdot 10 + 4 \cdot 10^2 + 3 \cdot 10^3 = 5 - 7 + 4 - 3,$$
$$86241 = 1 + 4 \cdot 10 + 2 \cdot 10^2 + 6 \cdot 10^3 + 8 \cdot 10^4 = 1 - 4 + 2 - 6 + 8.$$

Nennen wir also die Summe der mit abwechselndem Vorzeichen genommenen Ziffern — wobei die Einer das positive Zeichen bekommen — die *Querdifferenz* der Zahl, so haben wir:

Eine Zahl läßt bei der Teilung durch 11 denselben Rest wie ihre Querdifferenz; sie ist durch 11 dann und nur dann teilbar, wenn ihre Querdifferenz durch 11 teilbar ist.

5. Neuner- und Elferprobe.

Es ist:

$$455 \cdot 3217 = 1463735.$$

Den Rest, den dies Produkt bei der Teilung durch 9 (oder 11) läßt, können wir einmal finden, indem wir den Rest des Ergebnisses bestimmen, und dann auch so, daß wir den Rest der Faktoren berechnen und dann den Rest des Produktes dieser Reste bestimmen. Ist das Produkt richtig berechnet, so muß sich beidemal derselbe Wert ergeben.

Nach dem Modul 9 ist

$$1463735 = 1+4+6+3+7+3+5 = 29 = 2+9 = 11 = 1+1 = 2,$$
$$455 = 4+5+5 = 9+5 = 5,\ 3217 = 3+2+1+7 = 3+1+9 = 4,$$
$$455 \cdot 3217 = 5 \cdot 4 = 20 = 2+0 = 2.$$

Wir erhalten also als Rest beidemal 2.

Nach dem Modul 11 ist

$$1463735 = (5+7+6+1) - (3+3+4) = 19 - 10 = 9,$$
$$455 = (5+4) - 5 = 4,\ 3217 = (7+2) - (1+3) = 5,$$
$$455 \cdot 3217 = 4 \cdot 5 = 20 = 9,$$

so daß sich auch nach 11 beidemal derselbe Rest ergibt.

Es sei gerechnet:

$$a = 13 \cdot 28 \cdot 51 + 5 \cdot 213 - 17 \cdot 23 \cdot 35 = 5494.$$

Nach dem Modul 9 ist

$$13 \cdot 28 \cdot 51 = 4 \cdot 1 \cdot 6 = 24 = 6,\ 5 \cdot 213 = 5 \cdot 6 = 30 = 3,$$
$$17 \cdot 23 \cdot 35 = -1 \cdot 5 \cdot -1 = 5,\ a = 6 + 3 - 5 = 4$$

und andererseits

$$a = 5494 = 5 + 4 + 9 + 4 = 9 + 9 + 4 = 4.$$

Wir erhalten also auf beide Arten denselben Rest 4.

Nach dem Modul 11 ist

$$13 \cdot 28 \cdot 51 = 2 \cdot 6 \cdot -4 = 12 \cdot 7 = 1 \cdot 7 = 7, \quad 5 \cdot 213 = 5 \cdot 4 = 20 = 9,$$
$$17 \cdot 23 \cdot 35 = 6 \cdot 1 \cdot 2 = 1, \quad a = 7 + 9 - 1 = 15 = 4$$

und andererseits

$$a = 5494 = (4 + 4) - (9 + 5) = 8 - 14 = -6 = 5.$$

Wir erhalten also nicht auf beide Arten denselben Rest. Es ist daher falsch gerechnet.

Diese Rechenproben heißen die *Neuner-* und die *Elferprobe*. Geben beide ein richtiges Ergebnis, so *kann* richtig gerechnet sein; gibt aber auch nur eine ein falsches Ergebnis, so ist sicher falsch gerechnet — vielleicht bei einer der Proben.

Auf einen Fall sei besonders hingewiesen. Da eine Zahl bei der Teilung durch 9 denselben Rest läßt wie ihre Quersumme, so lassen zwei Zahlen, die sich nur durch die Anordnung der Ziffern unterscheiden, denselben Rest. Wenn man etwa bei einer Nebenrechnung eine Zahl insofern falsch schreibt, daß man ihre Ziffern vertauscht, z. B. 842 statt 824, so wird das Ergebnis falsch, aber die Neunerprobe stimmt. Wenn umgekehrt die Neunerprobe stimmt, die Elferprobe aber nicht, so kann man vermuten, daß man einen derartigen Fehler gemacht hat. Oder: Wenn ein Kassierer beim Kassenabschluß einen Überschuß oder Fehlbetrag findet, der durch 9 teilbar ist, so darf er vermuten, daß er einen Posten in der Art falsch eingetragen hat, daß er die Ziffern vertauscht hat, etwa 83 RM. 45 Pfg. statt 45 RM. 83 Pfg. oder 723 RM. statt 327 RM. Denn die Differenz zweier Zahlen mit derselben Quersumme ist immer durch 9 teilbar.

Frage: Warum sind 4 und 5 als Moduln ganz ungeeignet zu Rechenproben?

IV. Multiplikationstabellen.

1. Additionstabellen.

Rechnen wir nach dem Modul 7, so können wir uns auf die sieben Zahlen

(16) $$0, 1, 2, 3, 4, 5, 6$$

beschränken. In der Summe $a + b$ können a und b unabhängig voneinander die sieben Werte (16) annehmen, so daß wir im ganzen $7 \cdot 7$ Additionsaufgaben erhalten, deren Ergebnisse wir in einer quadratischen

Tabelle anordnen können. Wir schreiben über den oberen und vor den linken Rand der Tabelle die Zahlen (16) und bezeichnen die Zeilen nach den vor ihnen und die Spalten nach den über ihnen stehenden Zahlen, sprechen also von Zeile 0, Zeile 3, Spalte 6 usw. Das Ergebnis der Summe $a + b$ soll in der Tabelle dort stehen, wo Zeile a und Spalte b sich treffen. Wir erhalten so:

Tabelle für $a + b$.

Modul 7.

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Wir können aus dieser Additionstabelle (AT) auch die Werte für die Differenzen $b - a$ entnehmen. Wir setzen $b - a = c$ und betrachten die AT als Tabelle für die Summen $a + c = b$. Durch den ersten Summanden a ist uns die Zeile gegeben, in der die Summe b stehen muß. Die Spalte, in der sie sich befindet, gibt uns den gesuchten Summanden c oder die Differenz $b - a$. Beispiele: $3 - 5$. In Zeile 5 finden wir 3 in der Spalte 5, so daß $3 - 5 = 5$. In der Tat ist $5 + 5 = 3$ nach dem Modul 7. Oder: $2 - 6$. In Zeile 6 steht die 2 in Spalte 3, so daß $2 - 6 = 3$. Oder: $4 - 5$. In Zeile 5 befindet sich die 4 in Spalte 6, so daß $4 - 5 = 6$.

Dem Leser sei empfohlen, für weitere Moduln AT aufzustellen und sie zur Berechnung von Differenzen zu benutzen. Es ist das eine gute Vorübung für die folgenden wichtigeren und nicht so einfachen Multiplikationstabellen.

2. Multiplikationstabellen.

In derselben Weise wie AT können wir auch für verschiedene Moduln Multiplikationstabellen (MT) bilden. Der Unterschied ist nur der, daß dort, wo Zeile a und Spalte b sich treffen, jetzt der Wert des Produktes ab steht. Dabei sollen zunächst die positiv kleinsten Reste genommen werden, also beim Modul m die Zahlen

(17) $$0, 1, 2, \ldots, (m - 1).$$

Zur Herstellung der Tabellen sei folgendes gesagt. In Zeile 0 und Spalte 0 stehen nur Nullen, da dort der eine Faktor 0 ist. Die Zeile 1 enthält die Vielfachen von 1, also die Zahlen (17). Diese Zahlen gehen aus 0 hervor, indem wir fortgesetzt 1 addieren. Die Zeile 2 enthält die Vielfachen von 2. Wir erhalten sie, indem wir zu 0 wiederholt 2 addieren, wobei Vielfache von m gleich fortzulassen sind. Wir gehen also immer gleich um zwei Einheiten weiter statt um eine. Denken wir uns also die Zahlen der Zeile 1 in einem Kreise angeordnet, so erhalten wir aus ihnen die der Zeile 2, indem wir sie, bei 0 beginnend, mit 2 ab- oder auszählen, wobei die ausgezählten Zahlen immer wieder mit zu berücksichtigen sind. Allgemein enthält die Zeile a die Vielfachen von a, die wir erhalten, wenn wir zu 0 wiederholt a addieren, natürlich unter Fortlassung der Vielfachen von m. Wir schreiten daher in dieser Zeile immer um a Einheiten weiter, so daß wir diese Zeile aus Zeile 1 durch Auszählen mit a erhalten. Ferner: In Zeile 3 wird zu jeder Zahl 3 addiert, um die folgende zu erhalten; in Zeile 6 aber $6 = 3 + 3$ und in Zeile 9 immer $9 = 3 + 3 + 3$. Daher bekommt man die Zeilen 6 und 9 aus Zeile 3 durch Auszählen mit 2 und 3. Ebenso die Zeile 8 aus 4 durch Auszählen mit 2 und aus 2 durch Auszählen mit 4.

Zum Schluß sei noch eine Rechenkontrolle angegeben. Addieren wir zur letzten Zahl in Zeile a noch einmal a, so ergibt sich immer 0. Warum? Was würden wir überhaupt erhalten, wenn wir die Tabellen nach rechts weiter fortsetzen würden, wenn wir also nicht mit dem $(m-1)$-fachen von a aufhören würden, sondern auch noch das m-, $(m+1)$-, $(m+2)$-fache usw. hinschreiben würden, natürlich immer nach dem Modul m?

3. Tabellen.

Es folgen hier einige MT. Es wird dem Leser dringend empfohlen, sich diese Tabellen selbst herzustellen und auch noch weitere, etwa für die Moduln 19, 23, 24, 36.

Tabellen für $a \cdot b$.

Modul 5.

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Modul 6.

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Modul 7

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modul 8.

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Modul 9.

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Modul 10.

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Modul 11.

	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Modul 12.

	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

…enschaften der Tabellen.

1. … mit der Spalte *a* überein. Das kommt daher, daß bei… …n *a* in derselben Reihenfolge enthalten. Oder auch: Die Tabellen … …trisch zur Diagonale von links oben nach

rechts unten, zur sogenannten Hauptdiagonale. Als Grund kann man auch angeben: Es ist $a \cdot b = b \cdot a$.

2. Wir wollen uns in den Tabellen mal die Nullen in der ersten Zeile und Spalte, also die Randnullen, fortdenken. Es ist dann die letzte Zeile gleich der ersten in umgekehrter Reihenfolge. Das wird wohl jedem bei der Berechnung der Tabellen auffallen. Aber es ist auch die vorletzte Zeile gleich der zweiten in umgekehrter Reihenfolge. In derselben Beziehung stehen die dritte und die drittletzte Zeile usw. Entsprechendes gilt von den Spalten. Wir können diese Eigenschaft auch so ausdrücken: Nach Fortlassung der Randnullen sind die Tabellen symmetrisch zur Diagonale von links unten nach rechts oben, der sogenannten Nebendiagonale. Und der Grund hierfür? Wie wir wissen, entsteht z. B. die Zeile 2 aus der Zahl 0 durch wiederholtes Addieren von 2. Fügen wir zur letzten Zahl noch einmal 2 hinzu, so bekommen wir 0, und daher erhalten wir die Zahlen der Zeile 2 auch aus der Zahl 0 durch fortgesetzte Subtraktion von 2, aber in umgekehrter Reihenfolge, von rechts nach links. Die Zahlen der Reihe $m - 2$ gehen aus 0 hervor durch wiederholtes Addieren von $m - 2$ oder von -2, da $m - 2 = -2$ nach dem Modul m, also durch fortgesetztes Subtrahieren von 2. Sie entstehen daher aus 0 genau so wie die Zahlen der Zeile 2, aber in umgekehrter Reihenfolge. Oder: In der Zeile a steht in Spalte b das Produkt ab, und in Zeile $m-a$ steht in Spalte $m-b$ das Produkt $(m-a)(m-b)$, und das ist nach dem Modul m gleich $-a \; -b = ab$.

5. Division.

So wie wir eine AT zur Lösung von Subtraktionsaufgaben verwenden können, so können wir eine MT auch zur Lösung von Divisionsaufgaben benutzen. Wir verstehen dabei unter b/a die Zahl, die mit a multipliziert, b ergibt. Setzen wir $b/a = c$, so ist also $ac = b$. Von dem Produkt ac kennen wir den ersten Faktor a, und damit in der MT die Zeile, und das Ergebnis b, während der andere Faktor c, also die Spalte, gesucht. Haben wir uns daher für einen bestimmten Modul m en... wollen wir den Wert von b/a bestimmen, so haben wir ... entsprechenden MT in der Zeile a die Zahl b aufzusuchen. Steht sie ...palte c, so ist $b/a = c$. Der Leser möge sich, ehe er weiter liest, selbst Beispiele bilden und versuchen, sich die dabei auftretenden Merkwürdigkeiten zu erklären.

Hier seien nur einige Beispiele gegeben. *Modul 5:* $c = 2/3$. In Zeile 3 steht 2 in Spalte 4, so daß $2/3 = 4$. In der Tat ist $4 \cdot 3 = 12 = 2$ nach dem Modul 5. *Modul 11:* $c = 7/5$. In Zeile 5 steht 7 in Spalte 8, so daß $7/5 = 8$. Probe: $8 \cdot 5 = 40 = 7$. *Modul 10:* $c = 8/6$. In Zeile 6 steht 8

zweimal, nämlich in Spalte 3 und 8, so daß wir für 8/6 zwei Werte erhalten, nämlich 3 und 8. Es ist tatsächlich nach dem Modul 10 sowohl $3 \cdot 6$ wie auch $8 \cdot 6$ gleich 8. Für $c = 0/5$ ergeben sich sogar die fünf Werte 0, 2, 4, 6, 8. Oder es sei $c = 3/2$. In Zeile 2 findet sich keine 3, so daß die Aufgabe 3/2 nach dem Modul 10 keine Lösung hat.

Wir sehen, die Zahl b/a ist dann und nur dann vorhanden, wenn in Zeile a die Zahl b vorkommt, und wenn das $d$mal der Fall ist, so gibt es d Werte, und zwar *ganzzahlige*, für b/a. Es läßt sich also *jede* Zahl durch a dividieren, wenn in Zeile a *alle* Zahlen vorkommen. Da dann jede Zahl nur einmal vorkommen kann, so ist in diesem Falle die Division immer eindeutig. Wir heben den Fall $a = 0$, also die *Division durch* 0, besonders hervor. In Zeile 0 stehen nur Nullen, so daß $b/0$ nur vorhanden ist, wenn auch $b = 0$. Und 0/0 kann jede Zahl sein. Es ist ja auch für jedes c immer $c \cdot 0 = 0$. Wir sehen im folgenden von diesem Fall ab, setzen also den Nenner a immer als von 0 verschieden voraus.

In den Tabellen zu den Moduln 5, 7, 11 stehen in allen Zeilen, außer in Zeile 0, alle Zahlen. In den anderen Tabellen ist das nicht der Fall. Betrachten wir die Zeilen, die nicht alle Zahlen enthalten, genauer, so sehen wir, daß in ihnen die vorhandenen Zahlen *periodisch* wiederkehren (wie bei einem periodischen Dezimalbruch), und daß die in einer Periode enthaltenen Zahlen voneinander verschieden sind. Es ist nicht schwer zu sehen, daß das immer so sein muß. Da beim Modul m in Zeile a, wie in jeder Zeile, m Zahlen stehen, [illegible] müssen mindestens zwei gleiche vorkommen, wenn sie nicht alle vorkommen. Es sei $h = la$ die erste Zahl in Zeile a, die zum zweitenmal vorkommt. Es geht aber jede Zahl in Zeile a aus der folgenden durch Subtraktion von a hervor. Daher ist sowohl die vor dem ersten wie vor dem zweiten h stehende Zahl gleich $h-a$. Es würde daher die Zahl $h-a$ eher wiederkehren als h. Daraus folgt, daß in der Zeile a vor dem ersten h keine Zahl stehen darf, daß also das erste $h-a$ nicht zur Tabelle gehört. Mit anderen Worten, es muß h die erste [illegible] der Zeile, also 0 sein, so daß 0 die erste Zahl ist, die wiederkehrt. [illegible] das kleinste positive Vielfache von a, das 0 ist, so sind die [illegible] den der Zeile, nämlich

$$(18) \qquad 0,\ a,\ 2a, \ldots,\ (l-1)a$$

voneinander verschieden und bilden die *Periode*. Denn die nächste Zahl ist la, die gleich 0 ist, und da in Zeile a jede Zahl aus der vorhergehenden durch Addition von a entsteht, so folgen auf $la = 0$ die Zahlen a, $2a$, $3a$ usw., so daß die Zahlen (18) wiederkehren. Wir nennen die Anzahl l der in der Periode enthaltenen Zahlen die *Periodenlänge*.

Aus den Tabellen ersehen wir, daß jede Zeile durch eine volle Zahl von Perioden ausgefüllt wird. Daß das immer so sein muß, folgt einfach

daraus, daß auf die letzte Zahl jeder Zeile a das m-fache von a, also 0, folgt, so daß bei weiterer Fortsetzung der Tabellen dort eine neue Periode beginnt. Ist daher d die Anzahl der Perioden in Zeile a, so ist die Anzahl m der Zahlen in der Zeile gleich ld, so daß m durch l teilbar ist. Ferner ergibt sich, daß die Zahlen

$$0 \cdot a,\ l \cdot a,\ 2l \cdot a,\ 3l \cdot a, \ldots$$

und nur diese 0 sind. Es ist daher ein Vielfaches von a, etwa ha, dann und nur dann 0, wenn h durch l teilbar ist.

In der Tabelle des Moduls 10 haben die Zahlen der Zeile a für $a = 2$, 4, 6, 8 den g. g. T. 2, und 2 ist die Anzahl der Perioden und außerdem Teiler von a. Für $a = 5$ haben die Zahlen den g. g. T. 5, welche Zahl wieder gleich der Zahl d der Perioden ist und auch Teiler von a. In der Tabelle des Moduls 12 haben die Zahlen der Zeile a für $a = 3$ und 9 den g. g. T. 3, und 3 ist auch die Anzahl d der Perioden in diesen Zeilen und Teiler von a. Wir kommen so zu den beiden Vermutungen, daß die Anzahl d der Perioden in Zeile a nicht nur Teiler von m, sondern auch von a ist, und daß die Zahlen der Zeile a Vielfache von d sind.

Wir betrachten zunächst die erste Vermutung. Wie wir wissen, ist la durch m teilbar. Daher ist $la/m = la/ld = a/d$ eine ganze Zahl, so daß a tatsächlich Vielfaches von d ist. Es sei etwa $a = gd$, so daß

(19) $$m = ld,\quad a = gd.$$

Umgekehrt sei d' ein g. T. von m und a und es sei $m = l'd'$, $a = g'd'$. Dann ist nach dem Modul m

$$l'a = l'd'g' = mg' = 0.$$

Das gilt für jeden g. T. d' von a und m. Soll l' möglichst klein, also gleich l sein, so müssen wir d' möglichst groß wählen. Es ist daher d der g. g. T. von a und m. Und wir haben:

Die Länge l der Periode in Zeile a ist gleich m/d, wo d der g. g. T. (a, m) von a und m ist.

Die Länge der Periode in der Zeile a hängt also nicht von a selbst, sondern nur von d ab.

Ist $d = 1$, so ist $l = m$, und die Periode besteht aus allen m Zahlen. Sonst aber besteht die Periode nur aus $l < m$ Zahlen, und in der Zeile a kommt jede dieser Zahlen d mal vor. Unter diesen ist immer die 0, die ja die erste Zahl in jeder Zeile ist, und wir wollen zunächst sehen, was daraus folgt. Ist $d = 1$, ist also a teilerfremd zu m, so ist nur $0 \cdot a = 0$, und $0/a$ hat nur den einen Wert 0. Ist im besonderen m eine Primzahl p, so ist entweder a durch p teilbar, also 0 nach dem Modul p oder teilerfremd zu p. Daraus folgt: Ist nach p das Produkt ab gleich 0, so ist entweder $a = 0$ oder $b = 0$, da ja, wenn $a \neq 0$, nur $a \cdot 0 = 0$ ist. Sind daher

umgekehrt a und b beide nicht 0, so ist auch ab nicht 0. Ist c eine dritte von 0 verschiedene Zahl, so ist auch $(ab) \cdot c = abc$ nicht 0. So folgt:

Ist p eine Primzahl, so ist nach dem Modul p ein Produkt dann und nur dann 0, wenn mindestens ein Faktor 0 ist.

Das ist also genau so wie beim gewöhnlichen Rechnen. Es sei jetzt $d > 1$. Dann sind in der Zeile a genau d Zahlen 0, nämlich

$$(20) \qquad 0 \cdot a,\ l \cdot a,\ 2l \cdot a, \ldots, (d-1)l \cdot a,$$

und es hat $0/a$ die d Werte $0, l, 2l, \ldots, (d-1)l$. Es kann daher ein Produkt 0 sein, ohne daß ein Faktor 0 ist. So ist $4 \cdot 5$ nach 10 gleich 0. Oder nach 12 ist $4 \cdot 3 = 0$, $2 \cdot 3 \cdot 10 = 0$. Zwei Zahlen, die nicht 0 sind, deren Produkt aber 0 ist, heißen *Nullteiler*. Wir können also sagen:

Ist der Modul m eine zusammengesetzte Zahl, so gibt es Nullteiler.

Die gefundenen Sätze können wir auch in folgender Form aussprechen:

Ist $(a, m) = d$, $m = ld$ und ga durch m teilbar, so ist g Vielfaches von l. Im besonderen: Ist a teilerfremd zu m und ist ga durch m teilbar, so ist g durch m teilbar.

Ein Produkt ist durch eine Primzahl p dann und nur dann teilbar, wenn mindestens ein Faktor durch p teilbar ist.

Wir fügen noch hinzu: *Sind alle Faktoren eines Produktes zu m teilerfremd, so ist es auch das Produkt.*

Es sei nämlich etwa das Produkt $a_1 a_2 \cdots a_n = g$ nicht teilerfremd zu m, obwohl alle seine Faktoren es sind. Es sei p eine im g. g. T. von g und m enthaltene Primzahl. Dann ist g durch p teilbar und also auch mindestens einer der Faktoren a_i. Dieser wäre gegen die Voraussetzung nicht teilerfremd zu m. Wenn wir daher irgendwelche der Zahlen, die zu m teilerfremd sind, miteinander multiplizieren, so erhalten wir immer wieder eine dieser Zahlen.

Wir kehren zu unserer eigentlichen Aufgabe, der Division, zurück. Wie wir gesehen haben, ist eine Zahl b nach dem Modul m dann und nur dann teilbar durch a, wenn sie in der Zeile a der zugehörigen MT vorkommt, wenn sie also eine der l Zahlen (18) ist. In der Tabelle stehen aber nicht diese Zahlen selbst, sondern ihre Reste nach dem Modul m, und es ergibt sich die Frage, welche Zahlen das sind. Wir haben oben vermutet, daß es Vielfache der Anzahl d der in Zeile a enthaltenen Perioden sind. Das bestätigt sich. Denn zunächst sind die Zahlen (18) durch d teilbar, da sie Vielfache von a sind. Die in der Tabelle stehenden Zahlen unterscheiden sich aber von diesen nur durch Vielfache von m, und da auch m durch d teilbar ist, so sind es auch die in der Tabelle stehenden Zahlen. Die l in Zeile a stehenden Zahlen sind also unter den Zahlen

$$(21) \qquad 0,\ d,\ 2d, \ldots, (l-1)d$$

enthalten. Denn dies sind die einzigen Vielfachen von d, die nicht negativ sind und kleiner als m. Da aber die Anzahl der Zahlen (21) gerade l ist, so müssen sie alle vorkommen. Nach dem Modul m sind daher die Zahlen (18) mit den Zahlen (21), abgesehen von der Reihenfolge, identisch. Eine Zahl b findet sich also in Zeile a dann und nur dann, wenn sie durch d teilbar ist, und da sich die Zahlen der Zeile a $d$mal periodisch wiederholen, so kommt sie dann $d$mal vor, und zwar immer im Abstand l. Daher haben wir:

Nach dem Modul m ist eine Zahl b dann und nur dann durch eine Zahl a teilbar, wenn sie durch den g. g. T. $d = (a, m)$ von a und m teilbar ist, und es hat dann b/a genau d Werte. Ist der kleinste von diesen c, so ist

(22) $$b/a = c,\ c + l,\ c + 2l, \ldots, \text{ oder } c + (d-1)l.$$

Das gilt auch für $d = 1$ und $d = m$.

Aus (21) ersehen wir, daß nicht nur, wie wir schon früher gefunden haben, die Länge l der Periode, sondern auch die in der Periode enthaltenen Zahlen nicht von a selbst, sondern nur von d abhängen. In einer bestimmten Tabelle bestehen daher alle Perioden derselben Länge aus denselben Zahlen. So enthalten für den Modul 12 die Perioden der Länge l für $l = 6$ die geraden Zahlen, für $l = 4$ die Zahlen 0, 3, 6, 9 und für $l = 3$ die Zahlen 0, 4, 8. Außerdem sieht man, daß die Perioden der Länge l', wenn l' ein Teiler von l ist, nur Zahlen enthalten, die auch in den Perioden der Länge l vorkommen. Ist dir das aufgefallen, lieber Leser? Ist nämlich $l = l'h$ und $m = ld = l'd'$, so ist $d' = dh$, also ein Vielfaches von d, so daß die Vielfachen von d' unter denen von d enthalten sind. Dies alles folgt auch daraus, daß wir die Zeilen unserer Tabellen durch Auszählen mit einer passend gewählten Zahl aus Zeile 1 oder, unter Umständen, auch aus einer anderen Zeile erhalten, wie das oben erläutert ist.

6. Diophantische Gleichungen.

Es sei die Gleichung

(23) $$17x + 12y = 5$$

mit den Unbekannten x, y *ganzzahlig* zu lösen. Wir haben hier für die beiden Unbekannten nur *eine* Gleichung, aber die Bedingung, daß die Lösungen *ganze* Zahlen sein sollen. Derartige Gleichungen heißen nach dem griechischen Mathematiker Diophantes *diophantische Gleichungen*. Wir beschränken uns hier auf den allereinfachsten Fall solcher Gleichungen. Rechnen wir nach dem Modul 12, so folgt aus (23)

$$17x = 5x = 5,\ x = 1.$$

Das bedeutet, daß x sich von 1 nur durch ein Vielfaches von 12 unter-

scheiden darf. Es ist daher $x = 1 + 12u$, wo u irgendeine ganze Zahl ist. Setzen wir diesen Wert von x in (23) ein, so erhalten wir

$$17 + 17 \cdot 12u + 12y = 5, \text{ oder } 12y = -12 - 17u \cdot 12,$$

so daß sich die Lösung von (23) in der Form

$$x = 1 + 12u, \quad y = -1 - 17u$$

ergibt, wo u eine beliebige ganze Zahl ist. Für $u = 0$ erhalten wir z. B. $x = 1$, $y = -1$; für $u = 13$ wird $x = 157$, $y = -222$, was also auch eine Lösung von (23) ist.

Eine zweite Aufgabe sei

$$(24) \qquad 139x + 11y = 15.$$

Nach dem Modul 11 ist

$$139x = 7x = 15 = 4.$$

Aus der MT für den Modul 11 ersehen wir, daß $x = 4/7 = 10$. Daher können wir $x = 10 + 11u$ setzen, wo u eine ganze Zahl ist. Aus (24) folgt dann

$$1390 - 15 = 1375 = 11 \cdot 125 = -11y - 11 \cdot 139u,$$

so daß

$$x = 10 + 11u, \quad y = -125 - 139u$$

die Lösung von (24) ist.

Ein weiteres Beispiel sei

$$(25) \qquad 216x - 68y = 192.$$

Zunächst dividieren wir die Gleichung mit 4 und erhalten einfacher

$$(26) \qquad 54x - 17y = 48.$$

Nach dem Modul 17 folgt $54x = 3x = 48 = -3$, also $x = -1$. Wir können daher x in der Form $-1 + 17u$ annehmen. Dann folgt aus (26)

$$-54 - 48 = -102 = -6 \cdot 17 = 17y - 17 \cdot 54u.$$

Als Lösung von (25) finden wir daher

$$x = -1 + 17u, \quad y = -6 + 54u.$$

Z. B. ergibt sich für $u = 1$ die Lösung $x = 16$, $y = 48$.

Die Aufgabe

$$411x + 72y = 13$$

hat keine ganzzahlige Lösung. Warum nicht?

7. Einige Bemerkungen zu den Divisionsaufgaben nach einem Modul.

Es sei $x = b/a$ nach dem Modul m zu bestimmen. Wie wir gesehen haben, ist diese Aufgabe nur zu lösen, wenn b durch den g. g. T. d von a und m teilbar ist, und dann nach dem Modul m auf d Arten. Ist c ein Wert

von b/a, so sind die andern durch (22) gegeben, und es genügt, *eine* Lösung zu finden. Aber wie? Am einfachsten aus der MT für den Modul m. Die wird man jedoch nicht immer haben, und sie für vielleicht nur eine Aufgabe anzufertigen, lohnt nicht.

Es sei $b = b_0 d$. Wie wir in Nummer 3 des ersten Abschnittes gesehen haben, läßt sich jede Zahl des Ringes $\{a, m\}$, also im besonderen auch d, das die kleinste positive Zahl des Ringes ist, in der Form darstellen:

$$d = au + mv,$$

wo u und v ganze Zahlen sind. Diese Darstellung findet man, indem man die Herleitung der kleinsten Zahl des Ringes rechnerisch genau verfolgt. Wir gehen darauf nicht ein, wie man am schnellsten zum Ziele kommt. Multiplizieren wir die Darstellung von d mit b_0, so erhalten wir nach dem Modul m

$$b = b_0 d = a \cdot b_0 u, \quad x = b/a = b_0 u.$$

8. Division einer Gleichung nach einem Modul durch eine Zahl.

Beim gewöhnlichen Rechnen erhalten wir aus der Gleichung

$$fa = fb$$

für $f \neq 0$ wieder eine richtige Gleichung, wenn wir links und rechts mit f dividieren. Für $f = 0$ gilt das nicht. Z. B. geht die richtige Gleichung $4 \cdot 0 = 5 \cdot 0$ durch Division mit 0 in die falsche Gleichung $4 = 5$ über. Wie liegen die Verhältnisse beim Rechnen nach einem Modul m? Aus der gegebenen Gleichung folgt, daß $f(a-b)$ durch m teilbar ist. Ist $(f, m) = d$ und $m = dm'$, so ergibt sich nach Nummer 5 nur, daß $a-b$ durch m' teilbar sein muß. Also:

Ist $(f, m) = d$, $m = dm'$, so folgt aus $fa = fb$ nach dem Modul m, daß $a = b$ nach dem Modul m'.

Nur für $d = 1$ ist $m = m'$. Oder:

Rechnen wir nach dem Modul m, so dürfen wir eine Gleichung ohne weiteres durch eine zu m teilerfremde Zahl dividieren.

Ist m eine Primzahl, so ist jede von 0 verschiedene Zahl zu m teilerfremd, so daß wir für diesen Fall haben:

Rechnen wir nach einer Primzahl p als Modul, so dürfen wir jede Gleichung durch jede von 0 verschiedene Zahl dividieren.

Das ist genau so wie beim gewöhnlichen Rechnen.

Ist $d = m$, also f durch m teilbar und daher gleich 0 nach dem Modul m, so ist $fa = fb$ für beliebige Zahlen a und b. Es ergibt sich gar keine Bedingung für a und b.

V. Die Funktion $\varphi(n)$.

1. Die Definition.

In der MT für den Modul m kommen Perioden der Länge l vor, wenn l irgendein Teiler von m ist. Ist $m = ld$, so ist in einer Zeile a die Periodenlänge gleich l, wenn a mit m den g. g. T. d hat. Die Anzahl dieser Zeilen ist daher gleich der Anzahl derjenigen der m Zahlen von 0 bis $m-1$, die mit m den g. g. T. d haben. Ist $a = gd$ eine solche Zahl, so muß g zu l teilerfremd sein, und damit $a = gd$ eine der Zahlen von 0 bis $m-1$ ist, muß wegen $m = ld$ die Zahl g eine der Zahlen von 0 bis $l-1$ sein. Die Anzahl der Zeilen mit der Periodenlänge l ist daher auch gleich der Anzahl derjenigen unter den Zahlen von 0 bis $l-1$, die teilerfremd zu l sind. Ehe wir hieraus eine weitere Folgerung ziehen, betrachten wir allgemein *die Anzahl derjenigen Zahlen, die 0 oder positiv und kleiner als eine positive Zahl n sind, und die teilerfremd zu n sind.* Diese Zahl bezeichnet man nach Euler mit $\varphi(n)$. Für $n = 1$ bestehen die Zahlen von 0 bis $n-1$ nur aus der Zahl 0, und diese hat mit 1 den g. g. T. 1, so daß $\varphi(1) = 1$. Ist $n > 1$, so gehört 0 nicht zu den zu n teilerfremden Zahlen. Es ist daher für $n > 1$ $\varphi(n)$ die Anzahl der *positiven* Zahlen kleiner als n, die zu n teilerfremd sind. Für kleine n kann man ohne große Mühe die Zahl $\varphi(n)$ einfach dadurch bestimmen, daß man die Zahlen von 1 bis $n-1$ hinschreibt und nachsieht, wie viele zu n teilerfremd sind. So erhält man folgende Tabelle:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16

Ehe wir darauf eingehen, wie $\varphi(n)$ allgemein von n abhängt, wollen wir die Definition dieser Funktion etwas verallgemeinern. Wir gehen davon aus, daß eine zu n teilerfremde Zahl a zu n teilerfremd bleibt, wenn man zu ihr ein Vielfaches von n hinzufügt. Es gilt sogar allgemeiner der Satz:

Hat a mit n den g. g. T. d, so gilt dasselbe für jede Zahl a', die aus a durch Hinzufügen eines Vielfachen von n entsteht. Oder kürzer:

Alle Zahlen, die nach dem Modul n einander gleich sind, haben denselben g. g. T. mit n.

Das folgt einfach daraus, daß jeder g. T. von a und n auch g. T. von $a' = a + hn$ und n ist, und daß umgekehrt jeder g. T. von a' und n auch g. T. von $a = a' - hn$ und n ist. Wir können daher auch definieren:

Rechnen wir nach dem Modul n, so bedeutet $\varphi(n)$ die Anzahl derjenigen unter den dann nur vorhandenen n Zahlen, die teilerfremd zu n sind. Welches vollständige Restsystem wir dabei benutzen, ist gleichgültig.

2. Bestimmung von $\varphi(n)$, wenn n die Potenz einer Primzahl ist.

Ist zunächst n eine Primzahl p, so sind die Zahlen von 1 bis $p-1$ alle zu p teilerfremd, so daß

$$\varphi(p) = p - 1. \tag{27}$$

Es sei jetzt $n = p^\alpha$, wo p eine Primzahl ist. Anstatt die Anzahl derjenigen unter den Zahlen von 1 bis $n-1$ zu bestimmen, die zu n teilerfremd sind, berechnen wir umgekehrt die Anzahl derjenigen, die *nicht* zu n teilerfremd sind. Da n nur die Primzahl p enthält, so hat eine Zahl dann und nur dann mit n einen Teiler gemeinsam, wenn sie ein Vielfaches von p ist, wenn sie also die Form $a = pg$ hat. Soll a positiv und kleiner als n sein, so ist dazu notwendig und hinreichend, daß g positiv und kleiner als $n/p = p^{\alpha-1}$ ist, so daß g jede der Zahlen $1, 2, \ldots, p^{\alpha-1}-1$ sein kann. Daher ist die Anzahl derjenigen der Zahlen von 1 bis $n-1$, die nicht zu n teilerfremd sind, gleich $p^{\alpha-1}-1$, und es ist die Anzahl der anderen

$$n - 1 - (n/p - 1) = n - n/p = n\left(1 - \frac{1}{p}\right),$$

so daß

$$\varphi(p^\alpha) = \varphi(n) = n\left(1 - \frac{1}{p}\right). \tag{28}$$

3. Ein Satz über $\varphi(n)$.

Es sei $n = ab$, wo a und b echte Teiler von n sein sollen. Eine Zahl hat mit n keinen gemeinsamen Teiler dann und nur dann, wenn sie sowohl zu a wie zu b teilerfremd ist. Es ist aber eine der n Zahlen

$$0,\ 1,\ 2, \ldots, (n-1) \tag{29}$$

teilerfremd zu a, wenn der Rest, den sie bei der Teilung durch a läßt, zu a teilerfremd ist. Nach diesem Rest können wir die Zahlen (29) sehr schnell ordnen, indem wir sie der Reihe nach von links nach rechts in b Zeilen zu je a Zahlen schreiben. Für $a = 6$, $b = 5$, $n = ab = 30$ erhalten wir so

Tabelle 1.

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	26	27	28	29

In dieser Tabelle entsteht jede Zahl aus der über ihr stehenden durch Addition von 6, da man jedesmal um 6 weiterzählt, bis man von einer Zahl zu der darunter stehenden kommt. Daher sind die Zahlen jeder *Spalte* nach dem Modul $a = 6$ einander gleich. Wir bezeichnen die Spalten nach der in der ersten Zeile stehenden Zahl, also nach dem Rest, den die in der Spalte stehenden Zahlen bei der Teilung durch $a = 6$ lassen. Ebenso können wir die Zahlen (29) nach den Resten ordnen, die sie bei der Teilung durch b lassen. Wir wollen es aber diesmal so einrichten, daß die Zahlen jeder *Zeile* nach dem Modul b einander gleich werden. Dazu schreiben wir sie der Reihe nach von oben nach unten in a Spalten zu je b Zahlen. Für unser Beispiel erhalten wir so

Tabelle 2.

0	5	10	15	20	25
1	6	11	16	21	26
2	7	12	17	22	27
3	8	13	18	23	28
4	9	14	19	24	29

Wir bezeichnen in dieser Tabelle jede Zeile nach ihrer ersten Zahl, also nach dem Rest, den ihre Zahlen bei der Teilung durch $b = 5$ lassen.

Es liegt nahe, zu versuchen, die Zahlen (29) in einer Tabelle anzuordnen, die die beiden wesentlichen Eigenschaften von Tabelle 1 und 2 vereinigt. In dieser Tabelle von wieder a Spalten und b Zeilen müssen die Zahlen jeder Zeile nach dem Modul b und die jeder Spalte nach dem Modul a einander gleich sein. Es dürfen sich daher die Zahlen einer Spalte (Zeile) nur um Vielfache von a (b) unterscheiden, was z. B. der Fall ist, wenn wie in Tabelle 1 (2) die Zahlen jeder Spalte (Zeile) aus der ersten durch wiederholte Addition von a (b) hervorgehen. Eine derartige Tabelle von ab Zahlen können wir uns leicht herstellen, indem wir von 0 ausgehen, nach rechts immer b, nach unten immer a addieren und so ein Rechteck von a Spalten und b Zeilen ausfüllen. Aber die Frage ist, ob wir so die Zahlen (29) erhalten. Da es auf Vielfache von n bei unserer Frage nach den zu n teilerfremden Zahlen nicht ankommt, so können wir durch Subtraktion von n oder Vielfachen von n erreichen, daß die ab Zahlen unserer Tabelle alle unter den Zahlen (29) enthalten sind. Es fragt sich nun noch, ob in der Tabelle auch *alle* Zahlen (29) stehen, ob also die Zahlen der Tabelle alle voneinander verschieden sind. Wir nehmen zunächst zwei Beispiele. Es sei erstens wie oben $a = 6$, $b = 5$, $n = ab = 30$. Wir erhalten auf die angegebene Art, wenn wir gleich nach dem Modul 30 reduzieren, die

Tabelle 3.

0	5	10	15	20	25
6	11	16	21	26	1
12	17	22	27	2	7
18	23	28	3	8	13
24	29	4	9	14	19

Zweitens sei $a = 9$, $b = 6$, $n = ab = 54$. Wir erhalten (nach 54)

Tabelle 4.

0	6	12	18	24	30	36	42	48
9	15	21	27	33	39	45	51	3
18	24	30	36	42	48	0	6	12
27	33	39	45	51	3	9	15	21
36	42	48	0	6	12	18	24	30
45	51	3	9	15	21	27	33	39

Wir sehen: In Tabelle 3 stehen die $n = 30$ Zahlen von 0 bis 29, während in Tabelle 4 nicht alle $n = 54$ Zahlen von 0 bis 53 vorhanden sind, sondern nur durch 3 teilbare Zahlen. Das letzte ist klar. Denn die Zahlen 6 und 9, aus denen die Zahlen von Tabelle 4 durch wiederholtes Addieren gewonnen werden, haben den g. T. 3. Wir müssen daher auf jeden Fall voraussetzen, daß a und b teilerfremd sind. Aber das genügt auch, wie wir jetzt zeigen wollen. Die erste Zeile unserer Tabelle ist

$$0,\ b,\ 2b,\ 3b, \ldots,\ (a-1)b.$$

Diese Zahlen sind, wie wir von den MT her wissen, wegen $(a, b) = 1$, nach dem Modul a verschieden und stimmen, abgesehen von der Reihenfolge, mit den Zahlen von 0 bis $a-1$ überein. Die weiteren Zeilen der Tabelle entstehen dadurch, daß jede Zahl aus der darüber stehenden hervorgeht durch Addition von a. Die in einer Spalte stehenden Zahlen lassen daher bei der Teilung durch a alle denselben Rest, während Zahlen verschiedener Spalten auch einen verschiedenen Rest haben. Wir können und wollen die Spalten durch den positiv kleinsten Rest bezeichnen, den ihre Zahlen bei der Teilung durch a lassen. Was von den Spalten gilt, gilt aber auch von den Zeilen. Die erste Spalte enthält die Zahlen

$$0,\ a,\ 2a,\ 3a, \ldots,\ (b-1)a,$$

und diese sind nach dem Modul b in ihrer Gesamtheit gleich den Zahlen von 0 bis $b-1$. Und die Zahlen jeder Zeile sind nach dem Modul b einander gleich. Wir bezeichnen auch die Zeilen nach dem positiv kleinsten Rest, den ihre Zahlen bei der Teilung durch b lassen. Steht daher eine Zahl in Spalte α und in Zeile β, so läßt sie bei der Teilung durch a den Rest α und bei der Teilung durch b den Rest β. Und umgekehrt, wenn eine

der Zahlen von 0 bis $n-1$ bei der Teilung durch a und b die Reste α und β läßt, so findet man sie in der Tabelle da, wo Spalte α und Zeile β sich treffen. Daraus aber folgt, daß die $n = ab$ Zahlen der Tabelle voneinander verschieden sind, da keine zwei sowohl bei der Teilung durch a wie bei der durch b denselben Rest lassen können. Es sind daher in der Tabelle alle Zahlen von 1 bis $n-1$ und jede einmal enthalten. Da es unter den Zahlen von 0 bis $a-1$ $\varphi(a)$ zu a teilerfremde und unter den Zahlen von 0 bis $b-1$ $\varphi(b)$ zu b teilerfremde gibt, so sind in der Tabelle $\varphi(a)$ Spalten mit zu a und $\varphi(b)$ Zeilen mit zu b teilerfremden Zahlen vorhanden. Eine Zahl, die zu n, also zu a und zu b teilerfremd ist, muß aber gleichzeitig in diesen $\varphi(a)$ Spalten und $\varphi(b)$ Zeilen stehen. Ihre Anzahl ist daher gleich $\varphi(a)\cdot\varphi(b)$, so daß wir haben:

Ist $n = ab$, und sind a und b teilerfremd, so ist

(30) $$\varphi(n) = \varphi(ab) = \varphi(a)\cdot\varphi(b).$$

Wir schreiben die Tabelle 3 noch einmal hin, wobei wir über jede Spalte den Rest schreiben, den die Zahlen der Spalte bei der Division durch $a = 6$ lassen, und ebenso schreiben wir vor jede Zeile ihren Namen. Wir erhalten so

Tabelle 5.

	0	5	4	3	2	1
0	0	5	10	15	20	25
1	6	11	16	21	26	1
2	12	17	22	27	2	7
3	18	23	28	3	8	13
4	24	29	4	9	14	19

Die Tabellen 1, 2, 5 stehen in der Beziehung zueinander, daß die Zahlen, die in Tabelle 5 in Spalte α und in Zeile β sich finden, in Tabelle 1 in Spalte α und in Tabelle 2 in Zeile β stehen. Wir geben noch die den Tabellen 1, 2, 5 entsprechenden Tabellen für $a = 10$, $b = 9$, $n = ab = 90$ an.

Tabelle 6.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89

Tabelle 7.

0	9	18	27	36	45	54	63	72	81
1	10	19	28	37	46	55	64	73	82
2	11	20	29	38	47	56	65	74	83
3	12	21	30	39	48	57	66	75	84
4	13	22	31	40	49	58	67	76	85
5	14	23	32	41	50	59	68	77	86
6	15	24	33	42	51	60	69	78	87
7	16	25	34	43	52	61	70	79	88
8	17	26	35	44	53	62	71	80	89

Tabelle 8.

	0	9	8	7	6	5	4	3	2	1
0	0	9	18	27	36	45	54	63	72	81
1	10	19	28	37	46	55	64	73	82	1
2	20	29	38	47	56	65	74	83	2	11
3	30	39	48	57	66	75	84	3	12	21
4	40	49	58	67	76	85	4	13	22	31
5	50	59	68	77	86	5	14	23	32	41
6	60	69	78	87	6	15	24	33	42	51
7	70	79	88	7	16	25	34	43	52	61
8	80	89	8	17	26	35	44	53	62	71

In Tabelle 8 stehen in den $\varphi(10) = 4$ Spalten 1, 3, 7, 9 die zu 10 und in den $\varphi(9) = 6$ Zeilen 1, 2, 4, 5, 7, 8 die zu 9 teilerfremden Zahlen. Die $\varphi(10) \cdot \varphi(9) = 24$ Zahlen, die in beiden stehen, sind zu $10 \cdot 9 = 90$ teilerfremd, so daß $\varphi(90) = \varphi(10) \cdot \varphi(9) = 24$ wird.

Der über $\varphi(n)$ gefundene Satz läßt sich noch etwas verallgemeinern. Ist $n = abc$, wo a, b, c *zu je zweien* teilerfremd sind, so ist ab teilerfremd zu c und daher

$$\varphi(ab \cdot c) = \varphi(ab)\,\varphi(c) = \varphi(a)\,\varphi(b)\,\varphi(c).$$

So finden wir:

Ist $n = a_1 a_2 \cdots a_r$, und sind die Faktoren a_i zu je zweien teilerfremd, so ist

(31) $$\varphi(n) = \varphi(a_1)\,\varphi(a_2) \cdots \varphi(a_r).$$

4. Eine Formel für $\varphi(n)$ bei beliebigem n.

Es sei, in Primzahlen zerlegt,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Dann sind die Zahlen $p_i^{\alpha_i}$ zu je zweien teilerfremd, und durch Anwendung von (31) erhalten wir in Verbindung mit (28)

$$\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \varphi\left(p_2^{\alpha_2}\right) \cdots \varphi\left(p_r^{\alpha_r}\right)$$
$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right)$$

oder

(32) $$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Beispiele:

$$n = 300 = 2^2 \cdot 3 \cdot 5^2, \ \varphi(300) = 2^2 \cdot 3 \cdot 5^2 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 2^4 \cdot 5 = 80,$$

$$n = 1001 = 7 \cdot 11 \cdot 13, \ \varphi(1001) = 7 \cdot 11 \cdot 13 \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13} = 720,$$

$$n = 3072 = 2^{10} \cdot 3, \ \varphi(3072) = 2^{10} \cdot 3 \frac{1}{2} \cdot \frac{2}{3} = 2^{10} = 1024.$$

5. Eine Anwendung der Tabellen in Nr. 3.

Nehmen wir an, wir haben 30 Spielkarten, die wir uns in der Reihenfolge, in der sie gerade liegen, mit den Zahlen von 0 bis 29 bezeichnet denken. Wir bitten einen der Anwesenden, sich eine der Karten zu merken, und legen die Karten der Reihe nach in 5 Zeilen zu je 6, und zwar einmal von links nach rechts und einmal von oben nach unten, so daß wir die Tabellen 1 und 2 in Nummer 3 erhalten würden, wenn wir die Karten durch ihre Zahlen ersetzen. Wir fragen das erste Mal, in welcher Spalte, und das zweite Mal, in welcher Zeile die gemerkte Karte liegt. Ist das z. B. Spalte 5 und Zeile 2, so hat die Karte die Nummer, die in Tabelle 5 in Spalte 5 und Zeile 2 steht, also 17. Die gemerkte Karte ist daher die 17. Aber man muß mit 0 beginnen zu zählen.

Rein rechnerisch lautet diese Aufgabe so: Von einer der Zahlen von 0 bis 29 weiß man, welchen Rest sie bei der Teilung durch 6 und welchen sie bei der durch 5 läßt. Welche Zahl ist es? Die Reste seien z. B. 4 und 3. Die gesuchte Zahl muß in Tabelle 5 nach der von uns gewählten Bezeichnung der Spalten und Zeilen in Spalte 4 und Zeile 3 stehen. Es ist daher 28. In entsprechender Weise können wir Tabelle 8 verwenden. Eine Zahl lasse bei der Teilung durch 10 und 9 die Reste 5 und 6. Eine solche Zahl finden wir in Tabelle 8 in Spalte 5 und Zeile 6. Es ist 15.

6. Eine Aufgabe.

Die Betrachtungen der vorigen Nummer führen zu folgender Aufgabe. Es seien a und b zwei teilerfremde Zahlen. Es sollen alle Zahlen bestimmt werden, die durch a geteilt den Rest α und durch b geteilt den Rest β lassen, wo α und β zwei gegebene Zahlen sind.

$$(0 \leqq \alpha < a, 0 \leqq \beta < b).$$

Dieser Aufgabe können wir auch die Fassung geben: Es sollen alle Zahlen bestimmt werden, die nach dem Modul a gleich α und nach dem Modul b gleich β sind.

Beispiel 1: Es sei $a = 10$, $b = 9$, $\alpha = 4$, $\beta = 2$. Eine der gesuchten Zahlen finden wir in Tabelle 8 in Nr. 3. Sie muß dort gleichzeitig in Spalte 4 und Zeile 2 stehen. Sie ist daher 74. Eine andere Lösung sei x. Da x bei der Teilung durch 10 und 9 dieselben Reste lassen muß wie 74, so ist $x - 74$ sowohl durch 10 wie durch 9, also durch ihr k. g. V. 90 teilbar. Ist aber umgekehrt $x - 74$ durch 90 teilbar, so läßt x bei der Teilung durch 10 und 9 dieselben Reste wie 74. Daher ist $x - 74 = 90g$, wo g irgendeine Zahl ist, und die allgemeine Lösung unserer Aufgabe ist durch $74 + 90g$ gegeben. Für $g = -1$ erhalten wir z. B. die Lösung -16.

Beispiel 2: $a = 5$, $b = 13$, $\alpha = 4$, $\beta = 2$. Eine Tabelle steht uns hier nicht zur Verfügung. Die Zahlen einer solchen Tabelle würden hier alle aus 5 und 13 additiv zusammengesetzt sein, also die Form haben $5u + 13v$ mit ganzzahligem u und v. Es liegt nahe, die gesuchte Zahl

$$x = 5u + 13v \tag{33}$$

zu setzen und dann u und v passend zu bestimmen. Nach dem Modul 5 folgt aus (33) und aus der Aufgabe

$$13v = -2v = 4, \quad v = -2 = 3.$$

Nach dem Modul 13 ergibt sich entsprechend

$$5u = 2 = 15, \quad u = 3,$$

so daß

$$x = 5 \cdot 3 + 13 \cdot 3 = 54$$

eine Lösung unserer Aufgabe ist. Jede andere unterscheidet sich von dieser durch ein Vielfaches von $5 \cdot 13 = 65$, da für jede Lösung x die Differenz $x - 54$ durch 5 und durch 13 teilbar sein muß. Umgekehrt läßt jede Zahl, die sich von 54 um ein Vielfaches von 65 unterscheidet, bei der Teilung durch 5 und 13 dieselben Reste wie 54.

Beispiel 3: $a = 14$, $b = 27$, $\alpha = 11$, $\beta = 8$. Wir setzen $x = 14u + 27v$. Nach 14 wird

$$27v = -v = 11, \quad v = -11 = 3,$$

und nach 27 ist

$$14u = 8,\ 7u = 4,\ -20u = 4,\ 5u = -1 = -1 + 81 = 80,\ u = 16.$$

Eine Lösung ist daher $14 \cdot 16 + 27 \cdot 3 = 305$. Die allgemeine Lösung ist $x = 305 + 14 \cdot 27g = 305 + 378g$, wo g irgendeine Zahl ist.

Wir können diese Aufgaben in folgender Weise verallgemeinern. Es sollen die Zahlen bestimmt werden, die nach den gegebenen Moduln a, b, c die gegebenen Werte α, β, γ haben. Wir beschränken uns auf den Fall, wo die Zahlen a, b, c zu je zweien teilerfremd sind, wo also ihr k. g. V. gleich abc ist.

Nehmen wir an, wir hätten irgendeine Lösung x_0 unserer Aufgabe gefunden! Irgendeine andere Lösung sei x. Da dann x_0 und x bei der Teilung durch a, b, c dieselben Reste lassen, so ist $x - x_0$ durch a, b, c teilbar, also durch ihr k. g. V. abc. Hat umgekehrt $x - x_0$ diese Eigenschaft, so sind x und x_0 einander gleich nach den Moduln a, b, c. Ist daher x_0 irgendeine Lösung, so hat jede andere die Form

(34) $$x = x_0 + abc \cdot g,$$

wo g eine ganze Zahl ist.

Es liegt nahe, wie bei der vorigen Aufgabe, zunächst $x = au + bv + cw$ zu setzen. Nach dem Modul a würden wir dann haben $bv + cw = \alpha$, so daß wir immer noch zwei Unbekannte v und w hätten. Wir setzen daher besser

$$x = bcu + cav + abw.$$

Hieraus folgt:

Nach Modul a: $bcu = \alpha,\ u = \alpha/bc$;
nach Modul b: $cav = \beta,\ v = \beta/ca$;
nach Modul c: $abw = \gamma,\ w = \gamma/ab$.

Da wir voraussetzen, daß a, b, c zu je zweien teilerfremd sind, so sind die Divisionsaufgaben möglich. Denn die Nenner sind zu den jeweiligen Moduln teilerfremd.

Beispiel 1: $a = 3,\ b = 5,\ c = 7;\ \alpha = 2,\ \beta = 3,\ \gamma = 5$. Wir setzen

(35) $$x = 35u + 21v + 15w$$

und es wird

nach 3: $35u = 2u = 2,\ u = 1$;
nach 5: $21v = v = 3$;
nach 7: $15w = w = 5$,

so daß nach (35)

$$x_0 = 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 5 = 173$$

oder, da es auf ein Vielfaches von $abc = 105$ nicht ankommt, $x_0 = 68$. Es ist in der Tat

$$68 = 22 \cdot 3 + 2 = 13 \cdot 5 + 3 = 9 \cdot 7 + 5.$$

Nach (34) ist die vollständige Lösung

$$x = 68 + 105 \cdot g.$$

Beispiel 2: $a = 55$, $b = 12$, $c = 7$; $\alpha = 13$, $\beta = 5$, $\gamma = 5$; $abc = 4620$. Wir setzen

(36) $$x = 84u + 385v + 660w.$$

Nach Modul 55 wird $84u = 29u = 13$. Diese Gleichung zerlegen wir, indem wir einmal nach dem Modul 5 und dann nach 11 rechnen. Nach 5 ist $84 = -1$, $13 = 3$, also $u = -3 = 2$. Nach 11 wird $7u = 2$, $u = 2/7$. Aus der MT für den Modul 11 finden wir $u = 5$. Es ist daher u eine Zahl, die nach dem Modul 5 gleich 2 und nach 11 gleich 5 ist. Die Bestimmung von u erfordert daher die Lösung einer Aufgabe, wie wir sie im Anfang dieser Nummer betrachtet haben. Wir setzen

(37) $$u = 5r + 11s.$$

Nach Modul 5 folgt $11s = s = 2$, und nach 11 ist $5r = 5$, $r = 1$. Wegen (37) ist also $u = 27$.

Nach dem Modul 12 ergibt sich aus (36) $385v = v = 5$, und nach 7 folgt $660w = 2w = 5$, $w = 5/2 = 12/2 = 6$. Setzen wir die für u, v, w gefundenen Werte in (36) ein, so erhalten wir $x = 8153$. Da es auf Vielfache von $abc = 4620$ nicht ankommt, so ist auch 3533 eine Lösung unserer Aufgabe. In der Tat ist

$$3533 = 64 \cdot 55 + 13 = 294 \cdot 12 + 5 = 504 \cdot 7 + 5.$$

Die allgemeinste Lösung ist dann

$$x = 3533 + 4620 \cdot g,$$

wo g irgendeine Zahl ist.

7. Bemerkung zur Division nach einem Modul.

Die Aufgabe der Nummer 6 kann unter Umständen dazu benutzt werden, eine Division nach einem Modul auf einfachere Aufgaben zurückzuführen, nämlich auf Divisionen nach einem kleineren Modul. Wir erläutern das Verfahren an einem Beispiel. Es sei zu bestimmen

$$x = 502/327 \text{ nach dem Modul } 1001.$$

Es ist 1001 in die drei zu je zweien teilerfremden Faktoren 7, 11, 13 zerlegbar. Aus der Aufgabe folgt, daß

nach dem Modul 7:

$$327x = 5x = 502 = 5, \quad x = 1;$$

nach dem Modul 11:

$$327x = -3x = 502 = 7 = 18, \quad x = -6 = 5;$$

nach dem Modul 13:

$$327x = 2x = 502 = 8, \quad x = 4.$$

Unsere Aufgabe ist daher auf die Aufgabe zurückgeführt, eine Zahl x zu finden, die nach den Moduln 7, 11, 13 gleich 1, 5, 4 ist. Wir setzen, wie wir in der vorigen Nummer gelernt haben,

$$x = 143u + 91v + 77w. \tag{38}$$

Nach dem Modul 7 folgt hieraus $143u \equiv 3u \equiv 1 \equiv 15$, $u \equiv 5$; nach dem Modul 11 wird $91v \equiv 3v \equiv 5 \equiv 27$, $v \equiv 9 \equiv -2$; nach dem Modul 13 ist $77w \equiv -w \equiv 4$, $w \equiv -4$. Aus (38) ergibt sich schließlich

$$x \equiv 143 \cdot 5 - 91 \cdot 2 - 77 \cdot 4 \equiv 225 \equiv 502/327 \text{ nach dem Modul } 1001.$$

Probe: Es ist $225 \cdot 327 = 73575 = 502 + 73 \cdot 1001$.

Wir haben also die ursprüngliche Divisionsaufgabe nach dem Modul 1001 dadurch gelöst, daß wir sie auf Divisionsaufgaben nach den wesentlich kleineren Moduln 7, 11, 13 zurückgeführt haben. Denn sowohl die Bestimmung der Werte, die x nach diesen Moduln annimmt, wie auch die Berechnung von u, v, w führt auf Divisionsaufgaben. Das Verfahren ist immer anwendbar, wenn der Modul m der gegebenen Aufgabe sich in zu je zweien teilerfremde Faktoren zerlegen läßt, also nur dann nicht, wenn m eine Primzahl oder die Potenz einer solchen ist.

8. Noch ein Satz über $\varphi(n)$.

Wir betrachten wieder eine MT, und zwar die für den Modul n. In Nummer 1 dieses Abschnittes haben wir gesehen: Ist l ein Teiler von n, so gibt es in der Tabelle so viele Zeilen mit der Periodenlänge l, wie es unter den Zahlen von 0 bis $l-1$ zu l teilerfremde gibt, also $\varphi(l)$. Sind daher $l_1, l_2, \ldots, l_r$ die sämtlichen Teiler von n, mit Einschluß von 1 und n, so wird, da es im ganzen n Zeilen sind,

$$\varphi(l_1) + \varphi(l_2) + \cdots + \varphi(l_r) = n$$

oder in Worten:

Durchläuft l die sämtlichen Teiler einer Zahl n, wobei 1 und n eingeschlossen sind, so ist die Summe aller $\varphi(l)$ gleich n.

Beispiel 1: $n = 12$.

Teiler l	1	2	3	4	6	12
$\varphi(l)$	1	1	2	2	2	4

Es ist $1 + 1 + 2 + 2 + 2 + 4 = 12$.

Beispiel 2: $n = 16$.

Teiler l	1	2	4	8	16
$\varphi(l)$	1	1	2	4	8

Es ist $1 + 1 + 2 + 4 + 8 = 16$.

Beispiel 3: $n = 36$.

Teiler l	1	2	3	4	6	9	12	18	36
$\varphi(l)$	1	1	2	2	2	6	4	6	12

Es ist $1 + 1 + 2 + 2 + 2 + 6 + 4 + 6 + 12 = 36$.

VI. Der kleine Fermatsche Satz.

1. Die Potenzen einer Primzahl nach einer Primzahl als Modul.

In der MT für den Modul m stehen in der Zeile a die Vielfachen von a. Jede Zahl geht aus der vorhergehenden durch Addition und aus der folgenden durch Subtraktion von a hervor. Jede Zeile ist rein periodisch, und jede Periode beginnt mit 0. Ebenso können wir die Potenzen

(39) $$a^0 = 1,\ a^1,\ a^2, \ldots$$

einer Zahl a nach einem Modul aufschreiben. Es wird dem Leser empfohlen, sich schon hier Tabellen der Potenzen herzustellen. Sollte er dazu keine Lust haben, so vergleiche er zum Folgenden die Tabellen auf S. 38 und in VIII, 1. Wir beschränken uns auf den Fall, wo der Modul eine Primzahl p ist, und außerdem soll a nicht durch p teilbar sein, so daß $a \neq 0$ nach dem Modul p. An die Stelle der Addition tritt die Multiplikation, also an die Stelle der 0 die 1. In der Reihe (39) der Potenzen von a geht jede Zahl aus der vorhergehenden durch Multiplikation mit a hervor und auch jede aus der folgenden durch Division durch a. Denn da der Modul p eine Primzahl ist und $a \neq 0$, so ist die Division durch a eindeutig. Ferner sind die Zahlen (39) alle von 0 verschieden, so daß sie, wenn wir wieder die positiven kleinsten Reste wählen, unter den $p - 1$ Zahlen

(40) $$1,\ 2,\ 3, \ldots,\ p - 1$$

enthalten sind. Die Reihe (39) muß gerade so wie die Reihe der Vielfachen von a periodisch werden, und zwar rein periodisch, d. h. die erste Periode beginnt gleich mit der ersten Zahl. (Man erinnere sich an die rein periodischen Dezimalbrüche). Der Beweis ist genau so wie bei den Vielfachen von a. Denn da wir nur eine endliche Zahl von Zahlen haben, nämlich die $p - 1$ Zahlen (40), so muß mindestens eine Zahl zum zweitenmal auftreten. Es sei h die Zahl, die zum erstenmal wiederkehrt. Dann steht sowohl vor dem ersten wie vor dem zweiten h die Zahl h/a, und diese beiden Zahlen sind auch einander gleich, da die Division bei unseren Voraussetzungen eindeutig ist. Es würde also gegen die Annahme h/a

früher wiederkehren als h. Daraus folgt, daß vor dem ersten h keine Zahl stehen darf, daß also h die erste Zahl, d. h. $a^0 = 1$ sein muß. Es ist daher 1 die erste Zahl, die zum zweitenmal erscheint, und dann kommt wieder $a, a^2, a^3, \ldots$. Die Reihe (39) ist daher, wie behauptet, rein periodisch. Die Länge der Periode, d. h. die Zahl der in ihr enthaltenen Zahlen, bezeichnen wir wieder mit l. Es sind dann die Potenzen $a^0, a^l, a^{2l}, a^{3l}, \ldots$ und nur diese nach p gleich 1. Daher ist dann und nur dann $a^h = 1$ nach p für *jedes* positive a, wenn h durch *jede* Periodenlänge teilbar, also ein g. V. von ihnen ist. Bei der MT für den Modul m war das k. g. V. der Periodenlängen der m Zeilen gleich m. Wir *bezeichnen* hier das k. g. V. der $p-1$ Periodenlängen der $p-1$ Reihen (39), die wir für $a = 1, 2, \ldots, p-1$ erhalten, mit m. Machen wir uns eine Potenztabelle (PT), in der in Zeile a die Potenzen von a stehen, so stehen in Spalte m, d. h. in der Spalte, in der die m-ten Potenzen sich befinden, lauter Einsen, und es ist dies nach der Spalte 0 die erste, für die das eintritt. Um zu sehen, wie groß m ist, ob überhaupt m in einfacher Weise von p abhängt, betrachten wir Beispiele. Wir schreiben über eine Spalte die Zahl b, wenn in ihr die b-ten Potenzen stehen, und vor die Zeile der Potenzen von a setzen wir a. Wir erhalten so für $p = 5$ und $p = 7$:

Modul 5.

	0	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1	1
2	1	2	4	3	1	2	3	4
3	1	3	4	2	1	3	4	2
4	1	4	1	4	1	4	1	4

Modul 7.

	0	1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1	2	4	1
3	1	3	2	6	4	5	1	3	2	6
4	1	4	2	1	4	2	1	4	2	1
5	1	5	4	6	2	3	1	5	4	6
6	1	6	1	6	1	6	1	6	1	6

Es wird dem Leser empfohlen, weitere Beispiele zu rechnen. Wir gehen an späterer Stelle genauer auf PT ein. Hier kümmern wir uns nur um m. In den Beispielen ist $m = p - 1$. Weitere Beispiele würden dasselbe zeigen.

2. Der kleine Fermatsche Satz.

In der vorigen Nummer sind wir zu der Vermutung gekommen:

Ist p eine Primzahl, und rechnen wir nach dem Modul p, so ist für $a \neq 0$

(41) $$a^{p-1} = 1.$$

Dieser Satz ist, wie wir sehen werden, richtig. Er heißt der *kleine Fermatsche Satz*. Zum Beweise betrachten wir die MT für eine Primzahl als Modul, und zwar unter Weglassung der Nullen. Eine dieser Tabellen sei noch einmal angegeben, etwa die für den Modul 7, und zwar indem wir die Bezeichnung der Zeilen und Spalten fortlassen.

Modul 7.

1	2	3	4	5	6
2	4	6	1	3	5
3	6	2	5	1	4
4	1	5	2	6	3
5	3	1	6	4	2
6	5	4	3	2	1

In dieser Tabelle stehen in jeder Zeile die $p-1=6$ Zahlen von 1 bis $p-1$, und wir wissen von früher, daß das allgemein so ist, wenn der Modul eine Primzahl ist. Die Zeile 3 unserer Tabelle sagt, ausführlich geschrieben, daß nach dem Modul $p=7$

$$3 \cdot 1 = 3,\ 3 \cdot 2 = 6,\ 3 \cdot 3 = 2,\ 3 \cdot 4 = 5,\ 3 \cdot 5 = 1,\ 3 \cdot 6 = 4.$$

Multiplizieren wir diese Gleichungen miteinander, so erhalten wir bei passender Anordnung der Faktoren

$$3^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6.$$

Da keine der Zahlen 1 bis 6 gleich 0 ist, und da es Nullteiler bei einer Primzahl als Modul nicht gibt, so können wir mit diesen Zahlen dividieren und erhalten $3^6 = 1$.

Denselben Schluß können wir auch allgemein machen. Nach dem Modul p sind die Zahlen

(42) $$a \cdot 1,\ a \cdot 2,\ a \cdot 3, \ldots, a \cdot (p-1),$$

wenn p eine Primzahl ist, und wenn $a \neq 0$, gleich den Zahlen (40), wenn wir von der Reihenfolge absehen, so daß das Produkt der Zahlen (40) gleich dem der Zahlen (42) ist. Bezeichnen wir das Produkt der Zahlen von 1 bis $p-1$ mit g, so folgt

$$a^{p-1} \cdot g = g \text{ oder } (a^{p-1} - 1)g = 0.$$

Nach einer Primzahl als Modul ist aber ein Produkt nur 0, wenn mindestens einer seiner Faktoren 0 ist. Da keiner der in g enthaltenen Faktoren 0 ist, so ergibt sich die Gleichung (41) oder der kleine Fermatsche Satz.

3. Eine Verallgemeinerung.

Wir haben in der vorigen Nummer die MT für einen Modul p betrachtet unter Weglassung der durch p teilbaren Zahlen. Wir wollen jetzt allgemeiner die MT für einen beliebigen Modul m betrachten, unter Weglassung aller Zahlen, die einen gemeinsamen Teiler mit m haben. Es soll also nur das Produkt je zweier zu m teilerfremder Zahlen in die MT aufgenommen werden. Wie wir früher gesehen haben, ist ein solches Produkt wieder teilerfremd zu m, so daß in der Tabelle selbst auch nur die $\varphi(m)$ zu m teilerfremden Zahlen stehen. Hier sei nur die Tabelle für $m = 9$ angegeben. Weitere derartige Tabellen herzustellen, sei dem Leser überlassen.

Modul 9.

1	2	4	5	7	8
2	4	8	1	5	7
4	8	7	2	1	5
5	1	2	7	8	4
7	5	1	8	4	2
8	7	5	4	2	1

Die Bezeichnung der Zeilen und Spalten ist fortgelassen. Sie stimmt mit ihren ersten Zahlen überein, da dort der eine Faktor 1 ist. Wir sehen: In dieser Tabelle stehen, wie in der der vorigen Nummer, in jeder Zeile alle $\varphi(m) = \varphi(9) = 6$ Zahlen, die zu $m = 9$ teilerfremd sind. Das ist in jeder solchen Tabelle so. Wir wissen ja von früher, daß die Vielfachen von a vom 0-fachen bis zum $(m - 1)$-fachen nach dem Modul m voneinander verschieden sind, wenn a teilerfremd ist zu m. Da ferner hier in jeder Zeile nur zu m teilerfremde Zahlen vorkommen, so müssen sie alle vorkommen und voneinander verschieden sein. Die Zeile 5 unserer Tabelle sagt, ausführlich geschrieben, daß nach dem Modul $m = 9$

$$5 \cdot 1 = 5,\ 5 \cdot 2 = 1,\ 5 \cdot 4 = 2,\ 5 \cdot 5 = 7,\ 5 \cdot 7 = 8,\ 5 \cdot 8 = 4.$$

Bezeichnen wir das Produkt der Zahlen 1, 2, 4, 5, 7, 8 mit g, so folgt durch Multiplikation

$$5^6 g = 5^{\varphi(9)} g = g \text{ oder } (5^{\varphi(9)} - 1) g = 0.$$

Da g zu 9 teilerfremd ist, ergibt sich $5^{\varphi(9)} = 1$.

Allgemein sei $\varphi(m) = r$, und es seien

(43) $$a_1, a_2, \ldots, a_r$$

die r zu m teilerfremden Zahlen. Ferner sei a irgendeine der Zahlen (43). Dann sind die Zahlen

$$aa_1, aa_2, \ldots, aa_r$$

mit den Zahlen (43), abgesehen von der Reihenfolge, identisch. Es folgt daher durch Multiplikation, wenn wir das Produkt der Zahlen (43) mit g bezeichnen,

$$a^r g = a^{\varphi(m)} g = g \text{ oder } (a^{\varphi(m)} - 1) g = 0.$$

Da aber g zu m teilerfremd ist, so haben wir

(44) $$a^{\varphi(m)} = 1$$

und damit den Satz:

Ist a teilerfremd zu m, so ist $a^{\varphi(m)} = 1$ nach dem Modul m.

Der kleine Fermatsche Satz ist hierin enthalten. Ist nämlich m eine Primzahl p, so ist $\varphi(m) = p - 1$. Die Bedingung, daß $(a, m) = 1$ sein soll, ist notwendig. Wäre nämlich $(a, m) = d > 1$, und wäre die Differenz $a^{\varphi(m)} - 1$ durch m teilbar, also auch durch d, so würde folgen, daß der Subtrahend 1 durch d teilbar ist, da der Minuend $a^{\varphi(m)}$ es gewiß ist.

Für den Fall, daß m eine Primzahl p ist, kann man dem Satz die Fassung geben:

Ist p eine Primzahl, so ist nach dem Modul p für jede Zahl a

(44 a) $$a^p - a = a\,(a^{p-1} - 1) = 0.$$

Denn für $a = 0$ (nach p) ist der erste und für $a \neq 0$ der zweite Faktor 0. Und umgekehrt folgt aus (44 a), daß für $a \neq 0$ der zweite Faktor 0 sein muß, also der kleine Fermatsche Satz.

4. Eine weitere Verallgemeinerung.

Wir haben bei der Aufstellung der MT die positiv kleinsten Reste benutzt. Wir wollen jetzt MT aufschreiben unter Verwendung der absolut kleinsten Reste. Dabei beschränken wir uns auf den Fall, daß der Modul eine Primzahl p ist, und ferner lassen wir die 0 fort. Da das Produkt zweier von 0 verschiedenen Zahlen auch nicht 0 ist, so kommen dann nur die $p - 1$ Zahlen

$$-\frac{1}{2}(p-1),\ -\frac{1}{2}(p-3),\ \ldots,\ -1,\ 1,\ \ldots,\ \frac{1}{2}(p-3),\ \frac{1}{2}(p-1)$$

vor. *Beispiele:*

Modul 5. Reste: —2, —1, 1, 2.

	—2	—1	1	2
—2	—1	2	—2	1
—1	2	1	—1	—2
1	—2	—1	1	2
2	1	—2	2	—1

Modul 7. Reste: — 3, — 2, — 1, 1, 2, 3.

	— 3	— 2	— 1	1	2	3
— 3	2	— 1	3	— 3	1	— 2
— 2	— 1	— 3	2	— 2	3	1
— 1	3	2	1	— 1	— 2	— 3
1	— 3	— 2	— 1	1	2	3
2	1	3	— 2	2	— 3	— 1
3	— 2	1	— 3	3	— 1	2

Modul 13. Reste: ± 6, ± 5, ± 4, ± 3, ± 2, ± 1.

	—6	—5	—4	—3	—2	—1	1	2	3	4	5	6
—6	—3	4	—2	5	—1	6	—6	1	—5	2	—4	3
—5	4	—1	—6	2	—3	5	—5	3	—2	6	1	—4
—4	—2	—6	3	—1	—5	4	—4	5	1	—3	6	2
—3	5	2	—1	—4	6	3	—3	—6	4	1	—2	—5
—2	—1	—3	—5	6	4	2	—2	—4	—6	5	3	1
—1	6	5	4	3	2	1	—1	—2	—3	—4	—5	—6
1	—6	—5	—4	—3	—2	—1	1	2	3	4	5	6
2	1	3	5	—6	—4	—2	2	4	6	—5	—3	—1
3	—5	—2	1	4	—6	—3	3	6	—4	—1	2	5
4	2	6	—3	1	5	—4	4	—5	—1	3	—6	—2
5	—4	1	6	—2	3	—5	5	—3	2	—6	—1	4
6	3	—4	2	—5	1	—6	6	—1	5	—2	4	—3

Teilt man die Tabellen in vier gleiche Quadrate, so sieht man, daß in jedem von ihnen in jeder Spalte und in jeder Zeile, abgesehen vom Vorzeichen, die Zahlen $1, 2, \ldots, \frac{1}{2}(p-1)$ vorkommen. Wie das kommt, sieht man schon bei der Herstellung der Tabellen. Sobald man beim Berechnen einer Zeile über die Mitte hinauskommt, kehren dieselben Produkte in umgekehrter Reihenfolge und mit entgegengesetztem Vorzeichen wieder. Nehmen wir z. B. die Tabelle für den Modul 13 und die Vielfachen von -3. An erster Stelle steht $-3 \cdot -6$ und an letzter $-3 \cdot +6$. An zweiter Stelle steht $-3 \cdot -5$ und an zweitletzter $-3 \cdot +5$ usw. Zwei symmetrisch zur Mitte stehende Zahlen unterscheiden sich also nur durch das Vorzeichen. Ferner wissen wir, daß die in einer Zeile stehenden Zahlen alle voneinander verschieden sind. Kämen aber in einer Zeile in der ersten Hälfte zwei Zahlen vor, die sich nur durch das Vorzeichen unterscheiden,

etwa 2 und − 2, so würden in der zweiten Hälfte — 2 und 2 vorkommen, so daß in der ganzen Zeile 2 und — 2 doppelt vorhanden wären. Das aber kann nicht sein. Bedenken wir, daß die MT symmetrisch zur Hauptdiagonale sind, daß also alles, was von den Zeilen gilt, auch von den Spalten gilt, so ist die obige Behauptung über die Eigenschaft unserer Tabellen bewiesen.

Wir wenden die Schlußweise, die wir beim Beweis des kleinen Fermatschen Satzes benutzt haben, auf die rechten Hälften unserer neuen MT an. In der MT für den Modul 13 sagt die zweite Hälfte der Zeile 4, daß nach dem Modul 13

$$4 \cdot 1 \equiv 4,\ 4 \cdot 2 \equiv -5,\ 4 \cdot 3 \equiv -1,\ 4 \cdot 4 \equiv 3,\ 4 \cdot 5 \equiv -6,\ 4 \cdot 6 \equiv -2.$$

Da hier 4 Minuszeichen vorkommen, finden wir durch Multiplikation, wenn wir das Produkt der Zahlen von 1 bis 6 mit g bezeichnen,

$$4^6 g \equiv (-1)^4 g$$

oder, da g nicht durch 13 teilbar ist,

$$4^6 \equiv (-1)^4 \equiv 1.$$

Ebenso finden wir, daß nach dem Modul 13 für jede von 0 verschiedene Zahl a

$$a^6 \equiv (-1)^\lambda,$$

wenn λ die Zahl der in der rechten Hälfte der Zeile a vorhandenen negativen Zahlen ist.

Allgemein ergibt sich: Ist p eine ungerade Primzahl, und rechnen wir nach dem Modul p, so sind für $a \not\equiv 0$ die Zahlen

(45) $$a \cdot 1,\ a \cdot 2, \ldots,\ a \cdot \frac{1}{2}(p-1)$$

bis auf die Reihenfolge und das Vorzeichen identisch mit den Zahlen

(46) $$1,\ 2, \ldots,\ \frac{1}{2}(p-1).$$

Das Produkt der Zahlen (45) ist daher bis auf das Vorzeichen gleich dem der Zahlen (46). Bezeichnen wir also das Produkt der Zahlen (46) mit g, so ist

$$g a^{\frac{1}{2}(p-1)} \equiv (-1)^\lambda g$$

oder, da g ungleich 0 ist,

$$a^{\frac{1}{2}(p-1)} \equiv (-1)^\lambda.$$

Wir erhalten so die folgende Verallgemeinerung des Fermatschen Satzes:

Es sei p eine ungerade Primzahl. Rechnen wir nach dem Modul p, so ist für jede von 0 verschiedene Zahl a

(47) $$a^{\frac{1}{2}(p-1)} = (-1)^{\lambda}.$$

Dabei ist λ die Anzahl der negativen unter den absolut kleinsten Resten der Zahlen

(48) $$a,\ 2a,\ 3a, \ldots, \frac{1}{2}(p-1)a.$$

Aus (47) folgt durch Quadrieren wieder der Fermatsche Satz, daß $a^{p-1} = 1$ nach dem Modul p, wenn $a \neq 0$.

5. Über die Zahl λ.

Wir setzen zunächst zur Abkürzung

(49) $$\frac{1}{2}(p-1) = P.$$

Ferner beschränken wir uns auf *positive* Zahlen a. Die P Zahlen (48) sind von der Form ax, wo x eine der Zahlen (46) ist. Wollen wir eine von ihnen, etwa $a\alpha$, auf ihren absolut kleinsten Rest bringen, so bilden wir die Zahlen

(50) $$a\alpha,\ a\alpha - p,\ a\alpha - 2p,\ a\alpha - 3p, \ldots,$$

bis wir zu einer Zahl kommen, die zwischen $-P$ und $+P$ liegt, die Grenzen eingeschlossen. Eine und nur eine der Zahlen (50) hat diese Eigenschaft. Die Zahlen (50) haben die Form $a\alpha - py$, wo y eine nicht negative ganze Zahl ist. Uns kommt es nur auf die *negativen*, absolut kleinsten Reste an. Für diese ist sicher y größer als 0, da $a > 0$. Wir haben daher:

Es ist λ gleich der Anzahl derjenigen Zahlen der Form

(51) $$ax - py,$$

wo x eine der Zahlen von 1 bis P und wo $y > 0$, die zwischen -1 und $-P$ liegen, die Grenzen eingeschlossen. Wir betrachten Beispiele.

Beispiel 1: $a = 9,\ p = 7,\ P = 3.$

Die Zahlen (51) sind

$$\begin{array}{lll} 9\cdot1-7 = 2, & 9\cdot1-2\cdot7 = -5, & 9\cdot1-3\cdot7 = -12, \\ 9\cdot2-7 = 11, & 9\cdot2-2\cdot7 = 4, & 9\cdot2-3\cdot7 = -3, \\ 9\cdot3-7 = 20, & 9\cdot3-2\cdot7 = 13, & 9\cdot3-3\cdot7 = -6 \end{array}$$

usw. Wir erhalten diese Zahlen in Form einer Tabelle, indem wir mit $9-7$ beginnen und rechts neben jede Zahl die um 7 kleinere und unter jede die um 9 größere schreiben. Da x nur die Werte 1, 2, 3 annimmt, so enthält die Tabelle nur drei Zeilen. Da es uns nur darauf ankommt, wie viele Zahlen der Tabelle eine der Zahlen $-1, -2, -3$ sind, so

können wir in jeder Zeile aufhören, sobald eine Zahl erscheint, die kleiner ist als -3. Denn die Zahlen werden nach rechts immer kleiner. Die Tabellen sind also auch nach rechts begrenzt. Wir nehmen erst nochmal das

Beispiel 1: $a = 9$, $p = 7$, $P = 3$. Erste Zahl $9 - 7 = 2$.

2	— 5	— 12	— 19	— 26
11	4	— 3	— 10	— 17
20	13	6	— 1	— 8

In der Tabelle stehen zwei der Zahlen -1, -2, -3, so daß $\lambda = 2$. Daher ist $9^P = 9^3 = (-1)^2 = 1$ nach dem Modul 7. Probe: Es ist $9^3 = 2^3 = 8 = 1$ nach 7.

Beispiel 2: $a = 12$, $p = 7$, $P = 3 =$ Zahl der Zeilen. Erste Zahl $12 - 7 = 5$.

5	— 2	— 9	— 16	— 23	— 30	— 37
17	10	3	— 4	— 11	— 18	— 25
29	22	15	8	1	— 6	— 13

Diesmal finden wir nur eine der Zahlen -1, -2, -3 in der Tabelle, nämlich -2, so daß $\lambda = 1$ und $12^P = 12^3 = (-1)^1 = -1$ nach 7. In der Tat ist $12^3 = 5^3 = (-2)^3 = -8 = -1$.

Beispiel 3: $a = 5$, $p = 11$, $P = 5$. Es ist λ gleich der Anzahl der Zahlen, die gleich -1, -2, -3, -4 oder -5 sind. Erste Zahl $5 - 11 = -6$.

— 6	— 17	— 28
— 1	— 12	— 23
4	— 7	— 18
9	— 2	— 13
14	3	— 8

$\lambda = 2$. Daher $5^P = 5^5 = 1$ nach 11. Probe: $5^5 = 25 \cdot 25 \cdot 5 = 3 \cdot 3 \cdot 5 = 45 = 1$.

Beispiel 4: $a = 16$, $p = 13$, $P = 6$. Die Zahl λ gibt an, wie viele Zahlen gleich -1, -2, -3, -4, -5 oder -6 sind. Erste Zahl $16 - 13 = 3$.

3	— 10	— 23	— 36	— 49	— 62	— 75	— 88
19	6	— 7	— 20	— 33	— 46	— 59	— 72
35	22	9	— 4	— 17	— 30	— 43	— 56
51	38	25	12	— 1	— 14	— 27	— 40
67	54	41	28	15	2	— 11	— 24
83	70	57	44	31	18	5	— 8

$\lambda = 2$. Daher $16^P = 16^6 = (-1)^2 = 1$ nach 13. Probe: $16^6 = 3^6 = (3^3)^2 = 27^2 = 1^2 = 1$.

Beim Berechnen der Tabellen merkt man bald, daß man nicht alle Zahlen zu berechnen braucht, da es ja nur auf die Zahlen -1, -2, $-3, \ldots, -P$ ankommt. Nach rechts kann man aufhören, wie schon oben angegeben, wenn man zu einer Zahl kommt, die kleiner ist als $-P$, und nach unten, wenn eine positive Zahl auftritt. Dadurch vereinfacht sich die Bestimmung von λ bedeutend. Es ist aber darauf zu achten, daß die Anzahl der Zeilen nicht größer wird als $P = \frac{1}{2}(p-1)$. Wir bringen noch das

Beispiel 5: $a = 7$, $p = 13$, $P = 6$. Erste Zahl $7 - 13 = -6$.

[−6]	−19		
1	−12		
	[−5]	−18	
	2	−11	
		[−4]	−17
		3	−10

$\lambda = 3$, so daß $7^P = 7^6 \equiv (-1)^3 \equiv -1$ nach 13. Probe: $7^6 = (7^2)^3 = 49^3 \equiv 10^3 = 1000 \equiv -1$. (Es ist $1001 = 7 \cdot 11 \cdot 13$.)

Wir betrachten noch genauer den Fall, wo a eine *ungerade* Zahl ist, die wir mit q bezeichnen wollen. Die zugehörige Tabelle enthält die Zahlen $qx - py$, wo x die Werte $1, 2, \ldots, P = \frac{1}{2}(p-1)$ annimmt, so daß die Tabelle P Zeilen hat. Von y wissen wir, daß es eine positive Zahl ist. Da wir aber nur wissen wollen, wie viele der Zahlen der Tabelle zu den Zahlen von -1 bis $-P$ gehören, so brauchen wir y nur die Werte $1, 2, \ldots, Q$ annehmen zu lassen, wenn Q so gewählt wird, daß für jedes erlaubte x

$$qx - p(Q+1) < -P.$$

Das ist sicher dann der Fall, wenn die Ungleichung für den größten möglichen Wert von x, also für $x = P$ gilt, wenn also

$$qP - p(Q+1) < -P.$$

Hieraus folgt $(q+1)P < p(Q+1)$, also

$$p(Q+1) > (q+1)P$$

oder, wegen $P = \frac{1}{2}(p-1)$,

$$Q + 1 > \frac{p-1}{p} \cdot \frac{q+1}{2}.$$

Da $(p-1)/p$ ein echter Bruch ist, so ist diese Bedingung sicher erfüllt,

wenn wir $Q + 1 = \frac{1}{2}(q + 1)$, also $Q = \frac{1}{2}(q - 1)$ wählen, und das wollen wir tun. Da q ungerade ist, ist Q eine ganze Zahl. Wir haben daher:

Es sei p eine ungerade Primzahl und q eine ungerade Zahl. Es sei

(52) $$\frac{1}{2}(p-1) = P, \quad \frac{1}{2}(q-1) = Q$$

gesetzt. Ferner bedeute λ die Anzahl derjenigen unter den PQ Zahlen

(53) $$qx - py, \begin{cases} x = 1, 2, \ldots, P, \\ y = 1, 2, \ldots, Q, \end{cases}$$

die unter den Zahlen

(54) $$-1, -2, \ldots, -P$$

enthalten sind. Dann ist nach dem Modul p

(55) $$q^P \equiv (-1)^\lambda.$$

6. Der Fall $a = 2$.

Für $a = 2$ gelingt es, die Zahl λ für jedes p zu bestimmen. Wir benutzen dazu die ursprüngliche Bedeutung von λ. Danach ist λ die Anzahl derjenigen unter den P Zahlen

(56) $$1 \cdot 2,\ 2 \cdot 2,\ 3 \cdot 2, \ldots, P \cdot 2 = p - 1,$$

deren absolut kleinster Rest nach dem Modul p negativ ist. Die Zahlen (56) sind alle positiv und kleiner als p. Es sind die positiven geraden Zahlen unter p. Diejenigen, die kleiner als $p/2$ sind, gehören schon zu den absolut kleinsten Resten. Die anderen, die zwischen $p/2$ und p liegen, werden durch Subtraktion von p in absolut kleinste Reste verwandelt, und zwar in negative.

Beispiel 1: $p = 17$, $P = 8$. Die Zahlen (56) sind

$$2, 4, 6, 8, 10, 12, 14, 16.$$

Ihre absolut kleinsten Reste nach 17 sind

$$2, 4, 6, 8, -7, -5, -3, -1.$$

Beispiel 2: $p = 19$, $P = 9$. Die Zahlen (56) sind

$$2, 4, 6, 8, 10, 12, 14, 16, 18,$$

und ihre absolut kleinsten Reste sind

$$2, 4, 6, 8, -9, -7, -5, -3, -1.$$

Es ist daher λ auch die Anzahl derjenigen der Zahlen (56), die größer als $p/2$ sind. Wir unterscheiden zwei Fälle: I. P ist gerade, etwa $P = 2m$, also $p = 2P + 1 = 4m + 1$. II. P ist ungerade, etwa $P = 2m + 1$, also $p = 2P + 1 = 4m + 3$.

Fall I. $P = 2m$, $p = 4m + 1$.

In diesem Fall sind die ersten $\frac{1}{2}P = m$ der $P = 2m$ Zahlen (56) kleiner und die letzten m größer als $\frac{1}{2}p$. Denn es ist

$$2 \cdot m = P = \frac{1}{2}(p - 1) < \frac{1}{2}p,\ 2 \cdot (m + 1) = P + 2 = \frac{1}{2}(p + 3) > \frac{1}{2}p.$$

Daher ist im Fall I die Zahl λ gleich m. Nun kommt es uns nicht auf den Wert von λ selbst an, sondern auf den von $(-1)^\lambda$. Es ist aber $(-1)^\lambda$ gleich $+1$ oder -1, je nachdem λ gerade oder ungerade ist. Wir unterscheiden daher zwei Unterfälle:

I, 1: m ist gerade, $m = 2n$, $p = 4m + 1 = 8n + 1$. Es ist $\lambda = m$ gerade.

I, 2: m ist ungerade, $m = 2n + 1$, $p = 4m + 1 = 8n + 5$. Es ist λ ungerade.

Fall II. $P = 2m + 1$, $p = 4m + 3$.

Es sind wieder die ersten $\frac{1}{2}(P - 1) = m$ der Zahlen (56) kleiner als $\frac{1}{2}p$ und die übrigen, deren Anzahl diesmal $P - m = m + 1$ ist, größer. Denn es ist

$$2 \cdot m = P - 1 = \frac{1}{2}(p - 3) < \frac{1}{2}p,\ 2 \cdot (m + 1) = P + 1 = \frac{1}{2}(p + 1) > \frac{1}{2}p.$$

Es ist daher $\lambda = m + 1$. Wir unterscheiden wieder zwei Unterfälle:

II, 1: m ist gerade, $m = 2n$, $p = 4m + 3 = 8n + 3$. Es ist $\lambda = m + 1$ ungerade.

II, 2: m ist ungerade, $m = 2n + 1$, $p = 4m + 3 = 8n + 7$. Es ist $\lambda = m + 1$ gerade.

Damit haben wir gefunden: Es ist λ gerade, also $(-1)^\lambda = +1$, wenn p von der Form $8n + 1$ oder $8n + 7$ ist, wenn also p nach dem Modul 8 gleich 1 oder 7 ist, und es ist λ ungerade, also $(-1)^\lambda = -1$, wenn p von der Form $8n + 3$ oder $8n + 5$ ist, wenn also p nach dem Modul 8 gleich 3 oder 5 ist. Da $7 = -1$ und $5 = -3$ nach dem Modul 8, so können wir auch sagen:

Es ist $(-1)^\lambda = +1$, wenn $p = +1$ oder $p = -1$ nach dem Modul 8, wenn also p von der Form $8n \pm 1$ ist, und es ist $(-1)^\lambda = -1$, wenn $p = 3$ oder $p = -3$ nach 8, wenn also p die Form $8n \pm 3$ hat.

Damit sind aber alle Möglichkeiten erschöpft. Denn da p ungerade ist, so ist p nach 8 gleich einer der Zahlen $1, -1, 3, -3$. Aus dem in

Nr. 4 bewiesenen Satze folgt daher für den hier betrachteten Fall, wo $a = 2$ ist:

Nach dem Modul p ist, wenn p eine ungerade Primzahl bedeutet,

$$2^{\frac{1}{2}(p-1)} = +1, \text{ wenn } p = 8n \pm 1,$$

$$2^{\frac{1}{2}(p-1)} = -1, \text{ wenn } p = 8n \pm 3.$$

Im ersten Falle ist

$$\frac{1}{8}(p^2 - 1) = 8n^2 \pm 2n, \text{ also gerade,}$$

im zweiten

$$\frac{1}{8}(p^2 - 1) = 8n^2 \pm 6n + 1, \text{ also ungerade.}$$

Daher haben wir auch:

Ist p eine ungerade Primzahl, so ist nach dem Modul p

$$2^{\frac{1}{2}(p-1)} = (-1)^{\frac{1}{8}(p^2-1)}.$$

Beispiele:

1. $p = 7 = 8 \cdot 1 - 1,\ P = 3;\ 2^3 = 8 = +1.$
2. $p = 11 = 8 \cdot 1 + 3,\ P = 5;\ 2^5 = 32 = -1.$
3. $p = 17 = 8 \cdot 2 + 1,\ P = 8;\ 2^8 = 16 \cdot 16 = -1 \cdot -1 = 1.$
4. $p = 29 = 8 \cdot 4 - 3,\ P = 14;\ 2^{14} = 32 \cdot 32 \cdot 2^4 = 3 \cdot 3 \cdot 16 = 3 \cdot 48$ $= 3 \cdot -10 = -30 = -1.$

VII. Quadratische Reste.

1. Definition.

Es sei a eine positive Zahl. Wir betrachten die Reste, die die Quadratzahlen

$$1^2 = 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 16,\ 5^2 = 25, \ldots$$

bei der Teilung durch a lassen, welche der Zahlen

$$0,\ 1,\ 2, \ldots,\ a - 1 \tag{57}$$

also nach dem Modul a gleich Quadratzahlen sind. Zunächst ist klar, daß, wenn nach dem Modul a zwei Zahlen g und h einander gleich sind, dasselbe auch von ihren Quadraten g^2 und h^2 gilt (vgl. II, Nr. 3). Wir können uns daher auf die Quadrate der Zahlen (57) beschränken. *Dabei lassen wir die* 0 *fort.* Es sei z. B. $a = 10$. Die Quadrate sind

$$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81$$

und die Reste

$$1,\ 4,\ 9,\ 6,\ 5,\ 6,\ 9,\ 4,\ 1.$$

Es kommen also nicht alle Zahlen als Reste vor, sondern, abgesehen von 0, die wir ja immer fortlassen, nur 1, 4, 5, 6, 9, während 2, 3, 7, 8 fehlen. Daraus ergibt sich z. B., daß eine Zahl, deren letzte Ziffer 2, 3, 7 oder 8 ist, gewiß keine Quadratzahl ist. Wir nennen diejenigen Zahlen, außer 0, die nach dem Modul a gleich einer Quadratzahl sind, *quadratische Reste von a*, die anderen *quadratische Nichtreste von a*. Wir kürzen diese Bezeichnungen mit QR und QN ab.

2. Anzahl der QR und QN einer Primzahl.

Im Folgenden beschränken wir uns, wenigstens zunächst, auf den Fall, wo der Modul eine ungerade Primzahl p ist. Wir schreiben uns für die ersten Primzahlen die Reste der Quadrate der Zahlen von 1 bis $p - 1$ hin. Diese Zahlen stehen in den MT in der Hauptdiagonale.

$p = 3$. 1, 1.
$p = 5$. 1, 4, 4, 1.
$p = 7$. 1, 4, 2, 2, 4, 1.
$p = 11$. 1, 4, 9, 5, 3, 3, 5, 9, 4, 1.
$p = 13$. 1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1.
$p = 17$. 1, 4, 9, 16, 8, 2, 15, 13, 13, 15, 2, 8, 16, 9, 4, 1.
$p = 19$. 1, 4, 9, 16, 6, 17, 11, 7, 5, 5, 7, 11, 17, 6, 16, 9, 4, 1.

Wir sehen, jede Reihe ist symmetrisch zur Mitte. Das kommt einfach daher, daß $(-g)^2 = g^2$ ist. Nach dem Modul p ist $p - 1 = -1$, $p - 2 = -2$, $p - 3 = -3$ usw., so daß $(p-1)^2 = 1^2$, $(p-2)^2 = 2^2$, $(p-3)^2 = 3^2$ usw. Die Anzahl der QR ist daher höchstens gleich $\frac{1}{2}(p-1)$. Noch deutlicher sieht man das vielleicht, wenn man statt der Quadrate der Zahlen von 1 bis $p - 1$ die der absolut kleinsten Reste $\pm 1, \pm 2, \ldots, \pm \frac{1}{2}(p-1)$ benutzt. In den Beispielen sind die in den ersten Hälften jeder Reihe stehenden Zahlen voneinander verschieden, so daß die Zahl der QR genau gleich $\frac{1}{2}(p-1)$ ist. Auch das ist nicht schwer einzusehen, daß das immer so ist. Es seien nämlich g und $h < g$ zwei der Zahlen von 1 bis $\frac{1}{2}(p-1)$, und es sei nach p

$$g^2 - h^2 = (g-h)(g+h) = 0.$$

Dann müßte $g - h$ oder $g + h$ durch p teilbar sein, was sicher nicht der Fall ist. Denn diese beiden Zahlen sind beide positiv und kleiner als p. Damit haben wir:

Ist p eine ungerade Primzahl, so gibt es gleichviel QR und QN von p, nämlich je $\frac{1}{2}(p-1)$.

Wir haben ferner gesehen, daß ein QR immer das Quadrat von zwei Zahlen ist. Ist die eine g, so ist die andere $p-g$ oder, was nach p dasselbe ist, $-g$. Und diese beiden Zahlen sind immer (nach p) verschieden. Wir bezeichnen eine Zahl, deren Quadrat gleich a ist, auch mit Wurzel aus a, in Zeichen $\sqrt{a}$. Ist a ein QR, und ist zum Beispiel $a = g^2$, so ist

$$\sqrt{a} = \pm g.$$

Ist aber a ein QN, so existiert $\sqrt{a}$ nicht. So ist nach dem Modul 13: $\sqrt{4} = \pm 2$, $\sqrt{3} = \pm 4$, $\sqrt{12} = \pm 8$, während $\sqrt{5}$, $\sqrt{6}$ nicht vorhanden sind.

3. Produkte von QR und QN.

Um zu sehen, wie sich QR und QN verhalten, wenn man sie multipliziert, schreiben wir uns die MT, etwa für $p = 5$, 7 und 11, noch einmal auf, indem wir Zeilen und Spalten nach den QR und QN ordnen. Wir erhalten so:

Modul 5.

	1	4	2	3
1	1	4	2	3
4	4	1	3	2
2	2	3	4	1
3	3	2	1	4

Modul 7.

	1	2	4	3	5	6
1	1	2	4	3	5	6
2	2	4	1	6	3	5
4	4	1	2	5	6	3
3	3	6	5	2	1	4
5	5	3	6	1	4	2
6	6	5	3	4	2	1

Modul 11.

	1	3	4	5	9	2	6	7	8	10
1	1	3	4	5	9	2	6	7	8	10
3	3	9	1	4	5	6	7	10	2	8
4	4	1	5	9	3	8	2	6	10	7
5	5	4	9	3	1	10	8	2	7	6
9	9	5	3	1	4	7	10	8	6	2
2	2	6	8	10	7	4	1	3	5	9
6	6	7	2	8	10	1	3	9	4	5
7	7	10	6	2	8	3	9	5	1	4
8	8	2	10	7	6	5	4	1	9	3
10	10	8	7	6	2	9	5	4	3	1

Aus den Tabellen ersehen wir, daß die QR unter sich bleiben und ebenso die QN. Teilen wir die quadratischen Tabellen jede in vier kleinere Quadrate, so stehen im ersten und vierten die QR und im zweiten und dritten die QN. Das bedeutet aber:

Das Produkt aus zwei QR oder aus zwei QN ist ein QR. Das Produkt aus einem QR und einem QN ist ein QN.

Wir haben dies Ergebnis zu beweisen. Zunächst seien r_1 und r_2 zwei QR, also nach dem Modul p gleich Quadratzahlen, etwa $r_1 = a_1^2$, $r_2 = a_2^2$. Dann sind $r_1 r_2 = (a_1 a_2)^2$ und $r_1/r_2 = (a_1/a_2)^2$ auch Quadratzahlen. Es ist daher das Produkt und der Quotient zweier QR wieder ein QR. Da 1 immer QR ist, so ist im besonderen mit r auch $r^{-1} = 1/r$ ein QR. Es sei jetzt r ein QR und n ein QN. Wäre rn oder r/n oder n/r ein QR r', so würde der QN n gleich r/r' oder gleich r'/r oder gleich rr' sein, was alles dem eben Bewiesenen widerspricht. Daher ist das Produkt oder der Quotient eines QR und eines QN ein QN. Schließlich seien n_1 und n_2 zwei QN. Es sei, wie schon früher,

$$\frac{1}{2}(p-1) = P \tag{58}$$

gesetzt, und es seien

$$r_1, r_2, \ldots, r_P \tag{59}$$

die P QR von p. Die P Produkte

$$n_1 r_1, n_1 r_2, \ldots, n_1 r_P \tag{60}$$

sind voneinander nach dem Modul p verschieden und sind QN. Es sind daher die sämtlichen P QN von p. Dasselbe gilt von den P Quotienten

$$\frac{r_1}{n_1}, \frac{r_2}{n_1}, \ldots, \frac{r_P}{n_1}. \tag{61}$$

Daher kommt unter den Zahlen (60) und auch unter den Zahlen (61) die Zahl n_2 vor. Es sei etwa

$$n_2 = n_1 r_i \text{ und } n_2 = \frac{r_k}{n_1}. \tag{62}$$

Aus (62) folgt

$$\frac{n_2}{n_1} = r_i, \quad n_1 n_2 = r_k.$$

Das aber heißt: Das Produkt und der Quotient zweier QN ist ein QR. Damit ist unser Satz bewiesen.

4. Das Legendresche Symbol.

Das Ergebnis der vorigen Nummer können wir kurz so ausdrücken:

$$\text{QR} \cdot \text{QR} = \text{QR}, \quad \text{QR} \cdot \text{QN} = \text{QN}, \quad \text{QN} \cdot \text{QN} = \text{QR}.$$

Dies erinnert an

$$+1 \cdot +1 = +1, \quad +1 \cdot -1 = -1, \quad -1 \cdot -1 = +1.$$

Das hat Legendre dazu geführt, folgende Bezeichnung einzuführen:

Es sei p eine ungerade Primzahl und a eine durch p nicht teilbare ganze Zahl. Dann soll (a/p) die Zahl + 1 oder — 1 bedeuten, je nachdem a QR oder QN von p ist. Es heißt (a/p) das Legendresche Symbol. Es wird gelesen: a über p.

Wegen des angegebenen entsprechenden Verhaltens von QR und QN einerseits und + 1 und — 1 andererseits gilt

$$(63) \qquad \left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Da ferner jede Zahl, die nach dem Modul p einer Zahl a gleich ist, zugleich mit a QR oder QN ist, so gilt

$$(64) \qquad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right), \text{ wenn } a = b \text{ nach } p.$$

Nach der Zusammenstellung auf S. 50 ist zum Beispiel

$$\left(\frac{5}{11}\right) = 1, \quad \left(\frac{9}{13}\right) = 1, \quad \left(\frac{12}{17}\right) = -1, \quad \left(\frac{16}{19}\right) = 1, \quad \left(\frac{2}{19}\right) = -1.$$

Ferner wird zum Beispiel nach den beiden angegebenen Rechenregeln und nach der Zusammenstellung

$$\left(\frac{18}{11}\right) = \left(\frac{7}{11}\right) = -1 \text{ oder, auf andere Art,}$$

$$\left(\frac{18}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)^2 = \left(\frac{2}{11}\right) = -1.$$

$$\left(\frac{49}{13}\right) = \left(\frac{10}{13}\right) = 1 \text{ oder } \left(\frac{49}{13}\right) = \left(\frac{7}{13}\right)^2 = 1.$$

$$\left(\frac{72}{19}\right) = \left(\frac{2^3 \cdot 3^2}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{2}{19}\right)^2\left(\frac{3}{19}\right)^2 = \left(\frac{2}{19}\right) = -1.$$

Man kann offenbar in a enthaltene quadratische Faktoren ohne weiteres weglassen; das folgt ja auch schon daraus, daß jede Quadratzahl QR von p ist. So ist

$$\left(\frac{3^3 \cdot 5^2 \cdot 7^5}{17}\right) = \left(\frac{3 \cdot 7}{17}\right) = \left(\frac{21}{17}\right) = \left(\frac{4}{17}\right) = \left(\frac{2}{17}\right)^2 = 1.$$

5. Eine Formel für (a/p).

Wir betrachten die Tabelle für den Modul 11 auf S. 51, und zwar wollen wir uns die verschiedenen Zerlegungen einer Zahl in zwei Faktoren ansehen. Zunächst nehmen wir einen QN, etwa 7. Wir finden die Darstellungen

(65) $$7 = 1 \cdot 7,\ 7 = 3 \cdot 6,\ 7 = 4 \cdot 10,\ 7 = 5 \cdot 8,\ 7 = 9 \cdot 2.$$

Das sind $P = \frac{1}{2}(p-1) = 5$ Darstellungen, und es kommen in ihnen alle $p-1 = 10$ Zahlen von 1 bis 10 vor, und zwar jede einmal. Bezeichnen wir das Produkt der Zahlen von 1 bis $p-1$ mit g, setzen also

(66) $$1 \cdot 2 \cdot 3 \cdots (p-1) = g,$$

so folgt durch Multiplikation der Gleichungen (65)

$$7^P = 7^5 = g,$$

natürlich nach dem Modul 11. In derselben Weise finden wir nach dem Modul 11 für den QN 8 die Zerlegungen

$$8 = 1 \cdot 8,\ 8 = 3 \cdot 10,\ 8 = 4 \cdot 2,\ 8 = 5 \cdot 6,\ 8 = 9 \cdot 7$$

und hieraus durch Multiplikation

$$8^P = 8^5 = g.$$

Wir wählen jetzt einen QR von 11, etwa 3. Wir finden in der Tabelle folgende Zerlegungen von 3:

$$3 = 1 \cdot 3,\ 3 = 4 \cdot 9,\ 3 = 5 \cdot 5,\ 3 = 2 \cdot 7,\ 3 = 6 \cdot 6,\ 3 = 8 \cdot 10.$$

Wir erhalten diesmal sechs verschiedene Darstellungen. In diesen kommen auch wieder alle Zahlen von 1 bis $p-1 = 10$ vor, aber zwei, 5 und 6, doppelt. Das hängt damit zusammen, daß 3 nach dem Modul 11 eine Quadratzahl ist. Infolgedessen gibt es zwei Zahlen, die sich nur durch das Vorzeichen unterscheiden, deren Quadrat 3 ist, hier 5 und $6 = -5$. Ersetzen wir die beiden Gleichungen

$$3 = 5 \cdot 5,\quad 3 = 6 \cdot 6 = -5 \cdot -5$$

durch die eine

$$-3 = 5 \cdot -5 = 5 \cdot 6,$$

so haben wir die fünf Gleichungen

$$3 = 1 \cdot 3,\ 3 = 4 \cdot 9,\ 3 = 2 \cdot 7,\ 3 = 8 \cdot 10,\ -3 = 5 \cdot 6.$$

Durch Multiplikation erhalten wir:

$$-3^P = -3^5 = g.$$

Wir überlegen uns, warum das alles so ist. Wir rechnen nach einer ungeraden Primzahl p als Modul und denken uns die zugehörige MT unter Fortlassung der 0 aufgeschrieben. Irgendeine von 0 verschiedene Zahl s kommt in jeder Zeile einmal vor, im ganzen also $(p-1)$ mal.

Wir erhalten so $p-1$ Zerlegungen von s in zwei Faktoren. Es kommt aber s auch in jeder Spalte einmal vor. Da der erste Faktor die Zeile und der zweite die Spalte angibt, in der das Produkt steht, so sind die ersten Faktoren sowohl wie die zweiten die sämtlichen Zahlen von 1 bis $p-1$. In den $p-1$ Darstellungen von s als Produkt von zwei Zahlen kommen daher alle Zahlen von 1 bis $p-1$ vor, und zwar jede zweimal, nämlich einmal als erster und einmal als zweiter Faktor. Die MT ist aber symmetrisch zur Hauptdiagonale. Zwei Produkte, die symmetrisch zur Hauptdiagonale liegen, unterscheiden sich nur durch die Reihenfolge der beiden Faktoren, geben also im wesentlichen dieselbe Zerlegung von s. Wir müssen jetzt die beiden Fälle unterscheiden, wo s ein QN von p ist oder ein QR. Ist s ein QN, so kommt s in der Hauptdiagonale nicht vor, da ja in dieser gerade die QR stehen. Daher sind die $p-1$ Darstellungen von s paarweise einander gleich, und wir erhalten genau $P=\frac{1}{2}(p-1)$ verschiedene Zerlegungen

$$s=a_1a_2,\quad s=a_3a_4,\ \ldots,\quad s=a_{p-2}\,a_{p-1},$$

wo die Faktoren a_i die Zahlen von 1 bis $p-1$ sind. Durch Multiplikation folgt

(67) $$s^P=g.$$

Ist aber s ein QR, so kommt s wie jeder QR zweimal in der Hauptdiagonale vor. Das gibt für s zwei Zerlegungen mit gleichen Faktoren, etwa

(68) $$s=a_1a_1,\quad s=a_2a_2.$$

Es ist dann $a_2=-a_1$ nach dem Modul p, so daß wir wegen (68) auch haben

(69) $$-s=a_1\cdot -a_1=a_1a_2.$$

Die anderen Zerlegungen kommen wieder paarweise vor, und wenn wir von zwei gleichen immer nur eine beibehalten, so erhalten wir mit Einschluß von (69) die Darstellungen

$$-s=a_1a_2,\quad s=a_3a_4,\ \ldots,\quad s=a_{p-2}\,a_{p-1},$$

wo die Faktoren a_i wieder die Zahlen von 1 bis $p-1$ sind. Durch Multiplikation folgt

$$s^P=-g.$$

Damit haben wir bewiesen:

Es sei p eine ungerade Primzahl, und es bedeute g das Produkt der Zahlen von 1 bis $p-1$. Ferner sei $\frac{1}{2}(p-1)=P$ gesetzt. Es bedeute r irgendeinen QR und n einen QN von p. Dann ist nach dem Modul p

(70) $$r^P=-g,\quad n^P=g.$$

Da $1=1^2$ immer QR ist, so folgt im besonderen für $r=1$:

Ist p eine ungerade Primzahl, so ist nach dem Modul p

(71) $$g = 1 \cdot 2 \cdot 3 \cdots (p-1) = -1.$$

Das ist auch richtig für $p = 2$. Denn dann ist $g = 1$, und nach dem Modul 2 ist $1 = -1$. Es gilt aber ferner, daß die Gleichung (71) nur für Primzahlen richtig ist. Ist nämlich p eine zusammengesetzte Zahl, so hat p einen von 1 verschiedenen Teiler q, der kleiner ist als p, der also unter den Faktoren von g vorkommt. Wäre (71) auch in diesem Falle richtig, so wäre $g + 1$ durch p und daher auch durch q teilbar, während doch $g + 1$ bei der Teilung durch q den Rest 1 läßt, da q Teiler von g ist. Damit haben wir den *Wilsonschen Satz:*

Die ganze positive Zahl p ist dann und nur dann Primzahl, wenn

$$1 \cdot 2 \cdot 3 \cdots (p-1) + 1$$

durch p teilbar ist.

So ist, wenn wir für das Produkt der ganzen Zahlen von 1 bis n das Zeichen $n!$ (lies: n Fakultät) verwenden, $4! + 1 = 25$ durch 5, $6! + 1 = 721$ durch 7, $10! + 1 = 3\,628\,801$ durch 11 teilbar.

Nach dieser kleinen Abschweifung kehren wir zu den QR und QN zurück. Aus (70) und (71) folgt, daß $r^P = 1$ und $n^P = -1$ ist. Da auch $(r/p) = 1$ und $(n/p) = -1$, so haben wir den Eulerschen Satz:

Ist p eine ungerade Primzahl, so ist nach dem Modul p für jede von 0 verschiedene Zahl a

(72) $$\left(\frac{a}{p}\right) = a^{\frac{1}{2}(p-1)} = a^P.$$

Hierzu seien einige Bemerkungen gemacht. Nach dem Fermatschen Satz ist für $a \neq 0$ immer $a^{p-1} = 1$. Da $p - 1 = 2P$, so ist also nach dem Modul p

$$a^{p-1} - 1 = (a^P - 1)(a^P + 1) = 0.$$

Da p eine Primzahl ist, so muß einer der beiden Faktoren 0 sein, und es kann auch nur einer 0 sein. Denn sonst wäre ihre Differenz 2 gleich 0. Es ist daher für jede Zahl $a \neq 0$ entweder a^P gleich $+1$ oder -1. Es ist auch noch leicht zu sehen, daß das positive Zeichen gilt, wenn a ein QR ist. Ist nämlich $a = g^2$, so folgt durch Erheben zur P-ten Potenz $a^P = g^{2P} = g^{p-1}$, und das ist nach dem Fermatschen Satz $+1$. Nicht so leicht ergibt sich, daß $a^P = -1$ ist, wenn a ein QN ist, wie der durch (72) gegebene Satz aussagt. Nur wenn P eine ungerade Zahl ist, ist der Beweis einfach. Denn dann ist a^P als Produkt einer ungeraden Zahl von QN selbst ein QN und kann nicht gleich 1 sein, was ja ein QR ist. Da aber a^P nur einen der Werte $+1$ oder -1 haben kann, so muß a^P in diesem Falle gleich -1 sein. Außerdem zeigt sich, daß in dem Falle, wo P ungerade ist, -1 QN von p ist. Wir gehen nicht weiter hierauf ein und begnügen uns mit dem oben für (72) gegebenen Beweise.

6. Der Fall $a = -1$.

Wählen wir in (72) für a die Zahl -1, so folgt

$$\left(\frac{-1}{p}\right) = (-1)^P. \tag{73}$$

Ist also P gerade, etwa $P = 2m$ und $p = 4m + 1$, so ist $(-1/p) = +1$. Ist aber P ungerade, etwa $P = 2m + 1$ und $p = 4m + 3$, so ist $(-1/p) = -1$. Wegen der Bedeutung von $(-1/p)$ folgt:

Die Zahl -1 ist QR aller Primzahlen der Form $4m + 1$ und QN aller Primzahlen der Form $4m + 3$.

7. Der Fall $a = 2$.

In Abschnitt VI, Nr. 6 haben wir gesehen, daß

$$2^P = (-1)^{\frac{1}{8}(p^2-1)}$$

nach dem Modul p. In Verbindung mit (72) folgt für $a = 2$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)} \tag{74}$$

oder in Worten:

Die Zahl 2 ist QR aller Primzahlen von der Form $8n \pm 1$ und QN aller Primzahlen von der Form $8n \pm 3$.

Dieser Satz und der Satz der vorigen Nummer heißen *Ergänzungssätze zum quadratischen Reziprozitätsgesetz.* Diese Bezeichnung können wir erst später verstehen.

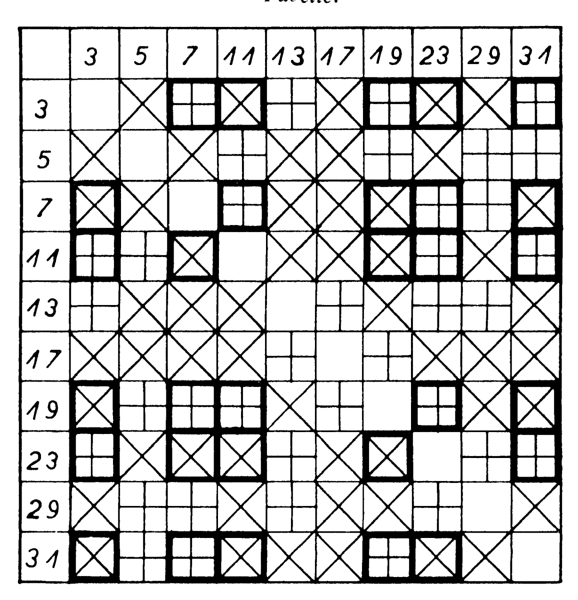
8. Das quadratische Reziprozitätsgesetz.

So einfach wie für -1 und 2 kann man für andere Zahlen nicht entscheiden, ob sie QR oder QN von einer Primzahl p sind. Wir stellen uns erst die Frage: Es seien p und q zwei ungerade Primzahlen. Ist dann q auch QR von p, wenn p QR von q ist? Oder allgemeiner: In welcher Beziehung stehen (q/p) und (p/q) zueinander? Gibt es überhaupt eine Beziehung zwischen diesen beiden Größen? Wir stellen uns zunächst eine Tabelle mit doppeltem Eingang her. Links und oben schreiben wir die ungeraden Primzahlen bis 31 hin. Wir bezeichnen die Zeilen und Spalten nach den Zahlen, die neben ihnen oder über ihnen stehen. Wir zeichnen dann in den Kreuzungspunkt von Zeile p und Spalte q für $p \neq q$ ein stehendes oder ein liegendes Kreuz, je nachdem (q/p) gleich $+1$ oder -1 ist. Für die Primzahlen bis 19 sind die QR auf S. 50 angegeben. Für 23, 29, 31 sind die QR

23: 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6.
29: 1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22.
31: 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8.

Die Diagonalfelder der Tabelle bleiben leer. In Zeile 3 steht also zunächst nichts, dann ×, da (5/3) = (2/3) = —1, dann +, da (7/3) = (1/3) = 1, dann ×, da (11/3) = (2/3) = —1 usw. In Zeile 13 steht + an erster Stelle, da (3/13) = 1, dann ×, da (5/13) = —1, dann ×, da (7/13) = —1, dann ×, da (11/13) = —1, dann bleibt ein Feld frei, dann +, da (17/13) = (4/13) = 1 usw. So erhalten wir die

Tabelle:



	3	5	7	11	13	17	19	23	29	31
3		×	**+**	**×**	+	×	**+**	**×**	×	**+**
5	×		×	+	×	×	+	×	+	+
7	**×**	×		**+**	×	×	**×**	**+**	+	**×**
11	**+**	+	**×**		×	×	**×**	**+**	×	**+**
13	+	×	×	×		+	×	+	+	×
17	×	×	×	×	+		+	×	×	×
19	**×**	+	**+**	**+**	×	+		**+**	×	**×**
23	**+**	×	**×**	**×**	+	×	**×**		+	**+**
29	×	+	+	×	+	×	×	+		×
31	**×**	+	**+**	**×**	×	×	**+**	**×**	×	

Wenn immer $(p/q) = (q/p)$ wäre, so müßte die Tabelle zur Hauptdiagonale symmetrisch sein. Daß das nicht der Fall ist, sieht man vielleicht am deutlichsten, wenn man die Figur so hält, daß diese Diagonale senkrecht steht. Es sind diejenigen Felder, die symmetrisch zur Diagonale liegen, und von denen das eine ein stehendes und das andere ein liegendes Kreuz enthält, stark umrahmt. Man sieht:

Die Zeilen und Spalten

(75) $$5, 13, 17, 29$$

sind frei von umrahmten Quadraten. Das bedeutet: Gehört auch nur eine der Primzahlen p, q zu den Zahlen (75), so ist $(p/q) = (q/p)$.

Alle Felder, abgesehen von den Diagonalfeldern, die nicht in einer der Zeilen oder in einer der Spalten (75) liegen, sind umrahmt. Oder: Alle Felder, die gleichzeitig in einer der Zeilen und Spalten

(76) $$3,\ 7,\ 11,\ 19,\ 23,\ 31$$

liegen, sind umrahmt. Es ist daher dann und nur dann $(p/q) = -(q/p)$, wenn p und q beide zu den Primzahlen (76) gehören.

Wodurch unterscheiden sich die Primzahlen (75) von den Primzahlen (76)? Die ersten lassen bei der Teilung durch 4 den Rest 1, die zweiten den Rest 3. So kommen wir zu der Vermutung:

Sind die ungeraden Primzahlen p und q beide von der Form $4n+3$, so ist $(p/q) = -(p/q)$. In allen anderen Fällen ist $(p/q) = (q/p)$.

Dieser Satz ist richtig und heißt das *quadratische Reziprozitätsgesetz.*

Da $\frac{1}{2}(p-1)$ und $\frac{1}{2}(q-1)$ gerade sind, wenn p und q bei der Teilung durch 4 den Rest 1 lassen, und ungerade, wenn p und q bei der Teilung durch 4 den Rest 3 lassen, so ist

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

dann und nur dann ungerade, wenn p und q beide von der Form $4n+3$ sind. Daher können wir das Reziprozitätsgesetz auch in der Form aussprechen:

Sind p und q zwei ungerade Primzahlen, so ist

(77) $$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Für die Anwendung ist die erste Form die bequemere.

9. Beweis des Reziprozitätsgesetzes.

Zum Beweise verwenden wir die Ergebnisse aus Abschnitt VI, Nr. 5 und benutzen auch die dort eingeführten Bezeichnungen. Wir haben dort gefunden:

Ist p eine ungerade Primzahl und q eine ungerade Zahl, so ist nach dem Modul p

$$q^P \equiv (-1)^\lambda,$$

wo λ folgende Bedeutung hat. Es ist λ die Anzahl derjenigen unter den PQ Zahlen

(78) $$qx - py, \quad \begin{cases} x = 1, 2, \ldots, P, \\ y = 1, 2, \ldots, Q, \end{cases}$$

die zwischen -1 und $-P$ liegen, die Grenzen eingeschlossen. Durch

Vergleich mit (72) folgt der Gaußsche Hilfssatz, nämlich daß

(79) $$\left(\frac{q}{p}\right) = (-1)^\lambda,$$

wo λ die eben angegebene Bedeutung hat. Ist auch q eine ungerade Primzahl, so gilt genau so:

Es ist

(80) $$\left(\frac{p}{q}\right) = (-1)^\mu;$$

dabei ist μ die Anzahl derjenigen unter den PQ Zahlen

(81) $$py - qx, \begin{cases} y = 1, 2, \ldots, Q, \\ x = 1, 2, \ldots, P, \end{cases}$$

die zwischen -1 und $-Q$ liegen, die Grenzen eingeschlossen. Da die Zahlen (78) und (81) sich nur durch das Vorzeichen unterscheiden, so ist μ auch die Anzahl derjenigen der Zahlen (78), die zwischen 1 und Q liegen, die Grenzen eingeschlossen. Aus (79) und (80) folgt

(82) $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\lambda+\mu} = (-1)^\nu.$$

Es ist $\nu = \lambda + \mu$ die Anzahl derjenigen der PQ Zahlen (78), die zwischen -1 und $-P$ oder zwischen 1 und Q liegen. Unter den Zahlen (78) kommt aber die 0 nicht vor. Denn aus $qx - py = 0$ würde folgen, daß zum Beispiel x durch p teilbar wäre, was nicht möglich ist, da x kleiner als p ist. Daher ist ν auch die Anzahl derjenigen der Zahlen (78), die zwischen $-P$ und $+Q$ liegen, die Grenzen eingeschlossen. Da es uns nur auf den Wert von $(-1)^\nu$ ankommt, so brauchen wir von ν nur zu wissen, ob es gerade oder ungerade ist. Um darüber Aufschluß zu bekommen, schreiben wir uns die Zahlen (78), wie in Abschnitt VI, Nr. 5, in einer Tabelle auf. Wir beginnen mit $q - p$ und schreiben rechts von jeder Zahl die um p kleinere und unter jede die um q größere, bis die Tabelle P Zeilen und Q Spalten hat. Wir geben einige Beispiele. Die im Intervall $-P$ bis $+Q$ liegenden Zahlen sind jedesmal stark umrahmt.

Beispiel 1: $p = 5$, $q = 7$; $P = 2$, $Q = 3$. Das Intervall von $-P$ bis $+Q$ enthält die Zahlen $-2, -1, 0, 1, 2, 3$.

2	−3	−8
9	4	1

Beispiel 2: $p = 5$, $q = 11$; $P = 2$, $Q = 5$. Das Intervall von $-P$ bis $+Q$ enthält die Zahlen $-2, -1, 0, 1, 2, 3, 4, 5$.

6	1	−4	−9	−14
17	12	7	2	−3

Beispiel 3: $p = 7$, $q = 11$; $P = 3$, $Q = 5$.

4	— 3	— 10	— 17	— 24
15	8	1	— 6	— 13
26	19	12	5	— 2

Beispiel 4: $p = 11$, $q = 13$; $P = 5$, $Q = 6$.

2	— 9	— 20	— 31	— 42	— 53
15	4	— 7	— 18	— 29	— 40
28	17	6	— 5	— 16	— 27
41	30	19	8	— 3	— 14
54	43	32	21	10	— 1

Es ist nicht notwendig, alle Zahlen zu berechnen. Ist eine Zahl zu groß, so ist jede unter ihr stehende erst recht zu groß, und ist eine Zahl zu klein, so ist jede rechts von ihr stehende erst recht zu klein.

Beispiel 5: $p = 13$, $q = 17$; $P = 6$, $Q = 8$.

4	— 9						
	8	— 5					
		12	— 1				
			16	3	— 10		
				20	7	— 6	
						11	— 2

Beispiel 6: $p = 19$, $q = 23$; $P = 9$, $Q = 11$.

4	— 15									
	8	— 11								
		12	— 7	— 26						
			16	— 3	— 22					
				20	1	— 18				
					24	5	— 14			
							9	— 10	— 29	
								13	— 6	— 25
									17	— 2

Die Anzahl der umrahmten Felder ist ν, und es kommt nur darauf an, ob ν gerade oder ungerade ist. Die Tabellen zeigen:

I. a. kommen die umrahmten Felder *paarweise* vor. Dreht man nämlich eine Tabelle um ihren Mittelpunkt um 180°, so kommen die rechts liegenden umrahmten Felder an die Stelle der links liegenden und umgekehrt. Oder: Zwei Felder, die gleichweit vom linken und vom rechten Rande und gleichzeitig auch vom oberen und unteren gleichweit entfernt sind, sind immer beide umrahmt oder beide nicht. Daher ist ν i. a. eine gerade Zahl. Es kann ν nur ungerade sein, wenn ein mittelstes Feld vorkommt, das bei der Drehung um 180° um den Mittelpunkt in sich selbst übergeht, das also keinen Partner hat. Und es ist in diesem Fall ν ungerade, wenn dies mittelste Feld umrahmt ist. Das ist in den, allerdings nur wenigen, Beispielen der Fall. Ein solches mittelstes Feld ist dann und nur dann vorhanden, wenn die Zahl der Zeilen und die der Spalten beide ungerade sind, wenn also $P = \frac{1}{2}(p-1)$ und $Q = \frac{1}{2}(q-1)$ ungerade Zahlen sind.

Gelten also die Eigenschaften unserer Tabellen allgemein, so ist ν dann und nur dann ungerade, wenn P und Q beide ungerade sind, wenn also PQ ungerade ist. Daraus würde dann folgen

$$(-1)^{\nu} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{83}$$

und wegen (82)

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{84}$$

oder auch, da (q/p) nur $+1$ oder -1 sein kann,

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right). \tag{85}$$

Das ist aber das Reziprozitätsgesetz.

Es bleibt zu zeigen, daß die benutzten Eigenschaften unserer Tabellen allgemein gelten. Die Zahl $qx - py$ steht in der Tabelle in der x-ten Zeile und in der y-ten Spalte. Es ist die erste Zeile soweit vom oberen Rande entfernt wie die P-te vom unteren. In derselben Beziehung stehen zueinander die zweite und die $(P-1)$-te Zeile, ebenso die dritte und die $(P-2)$-te usw. Es ist also von den Zahlen

$$g' = qx' - py', \quad g'' = qx'' - py'' \tag{86}$$

die erste soweit vom oberen Rande entfernt wie die zweite vom unteren, wenn

$$x' + x'' = P + 1. \tag{87}$$

Ähnlich folgt, daß die erste soweit vom linken Rande entfernt ist wie die zweite vom rechten, wenn

$$y' + y'' = Q + 1. \tag{88}$$

Unsere erste Vermutung geht dahin, daß die beiden Zahlen (86) unter Annahme der Gleichungen (87) und (88) entweder *beide* im Intervall

$$-P \text{ bis } +Q \tag{89}$$

liegen oder *beide* nicht. Die zweite Vermutung sagt aus: Wenn P und Q beide ungerade sind, so liegt die dann vorhandene mittelste Zahl

$$\begin{aligned} g_0 &= q\frac{P+1}{2} - p\frac{Q+1}{2} = (2Q+1)\frac{P+1}{2} - (2P+1)\frac{Q+1}{2} \\ &= \frac{1}{2}(2PQ + 2Q + P + 1 - 2PQ - 2P - Q - 1) = \frac{1}{2}(Q-P) \end{aligned} \tag{90}$$

im Intervall (89).

A M B

G_2'' $-P$ 0 G_1'' g_0 G_1' $+Q$ G_2'

Um die beiden Vermutungen zu beweisen, tragen wir auf der Zahlengeraden (siehe obige Figur), die den Zahlen $-P$ und $+Q$ entsprechenden Punkte A und B auf. Dem Mittelpunkt M von AB entspricht das Mittel der beiden Zahlen $-P$ und $+Q$, also die Zahl $\frac{1}{2}(-P+Q) = g_0$. Die zweite Vermutung ist daher sicher richtig. Wegen (86), (87), (88) und (90) ist das Mittel von g' und g''

$$\frac{1}{2}(g' + g'') = q\frac{P+1}{2} - p\frac{Q+1}{2} = g_0. \tag{91}$$

Der Punkt, der der Zahl $(g' + g'')/2$ entspricht, ist aber die Mitte der Strecke $G'G''$, wenn G' und G'' die Punkte sind, die den Zahlen g' und g'' entsprechen. Nach (91) ist die Mitte von $G'G''$ gleich der von AB. Daraus aber folgt, daß die Punkte G' und G'' entweder beide der Strecke AB angehören oder beide nicht. Das ist aber die erste Vermutung. Die Figur ist für $p = 13$, $q = 23$ gezeichnet. Die Punkte G_1', G_1'' entsprechen $x' = 3$, $y' = 5$ und G_2', G_2'' $x' = 4$, $y' = 6$.

Damit ist das quadratische Reziprozitätsgesetz bewiesen.

10. Die Berechnung von (a/p).

Zunächst stellen wir die Sätze zusammen, die wir zur Berechnung von (a/p) verwenden.

1. Es ist $(a/p) = (a'/p)$, wenn $a \equiv a'$ nach dem Modul p.

2. Es ist

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \quad \left(\frac{abc}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right) \text{ usw.} \tag{92}$$

3. Man kann in a enthaltene quadratische Faktoren fortlassen.

4. Es ist $(1/p) = 1$.

5. Es ist $(-1/p)$ gleich $+1$ oder -1, je nachdem p die Form $4n+1$ oder $4n-1$ hat.

6. Es ist $(2/p)$ gleich $+1$ oder -1, je nachdem p die Form $8n \pm 1$ oder $8n \pm 3$ hat.

7. Ist q eine von p verschiedene ungerade Primzahl, so ist $(p/q) = -(q/p)$, wenn p und q beide von der Form $4n-1$ sind. Sonst ist $(p/q) = (q/p)$.

Diese Regeln können in folgender Weise zur Berechnung von (a/p) benutzt werden. Wegen 1. können wir a durch den positiv oder absolut kleinsten Rest nach p ersetzen, etwa durch b. Es ist dann b positiv und kleiner als p, oder es liegt zwischen $-p/2$ und $+p/2$. So ist $(95/17) = (10/17) = (-7/17)$, $(357/59) = (3/59)$, $(378/101) = (75/101)$, $(40/41) = (-1/41)$. Dann zerlegt man b in Primfaktoren und erhält nach 2. für (b/p) ein Produkt von Legendreschen Symbolen, deren obere Zahlen -1, 2 oder eine ungerade Primzahl sind. Dabei kann man nach 3. quadratische Faktoren von b gleich fortlassen. So wird $(10/17) = (2/17)\cdot(5/17)$, $(-7/17) = (-1/17)\cdot(7/17)$, $(15/59) = (3/59)\cdot(5/59)$, $(75/11) = (5^2\cdot 3/11) = (3/11)$. Manchmal kann man auch vorteilhaft gleich die Regel 2 anwenden, besonders dann, wenn a einen quadratischen Faktor enthält. So ist $(2\cdot 3^3\cdot 5^4/97) = (2\cdot 3/97) = (2/97)\cdot(3/97)$, $(529/43) = (23^2/43) = 1$. Auch kommt man manchmal eher zum Ziel, wenn man a nicht gerade durch den kleinsten Rest ersetzt, sondern durch eine andere Zahl, die ihr nach dem Modul p gleich ist. So ist $(185/11) = (196/11) = (14^2/11) = 1$, $(957/43) = (1000/43) = (10^2\cdot 10/43) = (10/43) = (2/43)\cdot(5/43)$.

Der Wert der etwa vorkommenden Faktoren $(-1/p)$ und $(2/p)$ ergibt sich aus Regel 5 und 6. In den anderen Faktoren (q/p) ist q eine ungerade Primzahl, die kleiner ist als p. Nach Regel 7 ersetzen wir (q/p) durch (p/q) oder $-(p/q)$. In (p/q) können wir dann wieder nach Regel 1 die obere Zahl p durch ihren Rest nach q ersetzen, so daß wir kleinere Zahlen bekommen. So wird die Aufgabe der Berechnung von (a/p) auf Aufgaben derselben Art, aber in kleineren Zahlen zurückgeführt. Das Verfahren kann man fortsetzen, bis man zu Legendreschen Symbolen kommt, deren obere Zahl 1, -1 oder 2 ist, und deren Werte man nach Regel 4, 5 und 6 angeben kann.

Beispiele:

$$\left(\frac{200}{61}\right)=\left(\frac{2^3 5^2}{61}\right)=\left(\frac{2}{61}\right)=-1 \text{ oder}$$

$$\left(\frac{200}{61}\right)=\left(\frac{17}{61}\right)=\left(\frac{61}{17}\right)=\left(\frac{10}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{5}{17}\right)=\left(\frac{5}{17}\right)=\left(\frac{17}{5}\right)$$
$$=\left(\frac{2}{5}\right)=-1.$$

$$\left(\frac{135}{61}\right)=\left(\frac{3^3\cdot 5}{61}\right)=\left(\frac{3}{61}\right)\left(\frac{5}{61}\right)=\left(\frac{61}{3}\right)\left(\frac{61}{5}\right)=\left(\frac{1}{3}\right)\left(\frac{1}{5}\right)=1 \text{ oder}$$

$$\left(\frac{135}{61}\right)=\left(\frac{13}{61}\right)=\left(\frac{61}{13}\right)=\left(\frac{3^2}{13}\right)=1 \text{ oder}$$

$$\left(\frac{135}{61}\right)=\left(\frac{196}{61}\right)=\left(\frac{14^2}{61}\right)=1.$$

$$\left(\frac{133}{59}\right)=\left(\frac{7}{59}\right)\left(\frac{19}{59}\right)=-\left(\frac{59}{7}\right)\cdot-\left(\frac{59}{19}\right)=\left(\frac{3}{7}\right)\left(\frac{2}{19}\right)=-\left(\frac{7}{3}\right)\cdot-1$$
$$=\left(\frac{7}{3}\right)=\left(\frac{1}{3}\right)=1 \text{ oder}$$

$$\left(\frac{133}{59}\right)=\left(\frac{15}{59}\right)=\left(\frac{3}{59}\right)\left(\frac{5}{59}\right)=-\left(\frac{59}{3}\right)\left(\frac{59}{5}\right)=-\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)=1 \text{ oder}$$

$$\left(\frac{133}{59}\right)=\left(\frac{-44}{59}\right)=\left(\frac{-1}{59}\right)\left(\frac{11}{59}\right)=\left(\frac{59}{11}\right)=\left(\frac{4}{11}\right)=1.$$

$$\left(\frac{52}{53}\right)=\left(\frac{4\cdot 13}{53}\right)=\left(\frac{13}{53}\right)=\left(\frac{53}{13}\right)=\left(\frac{1}{13}\right)=1 \text{ oder}$$

$$\left(\frac{52}{53}\right)=\left(\frac{-1}{53}\right)=1.$$

$$\left(\frac{253}{257}\right)=\left(\frac{11}{257}\right)\left(\frac{23}{257}\right)=\left(\frac{257}{11}\right)\left(\frac{257}{23}\right)=\left(\frac{4}{11}\right)\left(\frac{4}{23}\right)=1 \text{ oder}$$

$$\left(\frac{253}{257}\right)=\left(\frac{-4}{257}\right)=\left(\frac{-1}{257}\right)=1.$$

$$\left(\frac{111}{131}\right)=\left(\frac{3\cdot 37}{131}\right)=\left(\frac{3}{131}\right)\left(\frac{37}{131}\right)=-\left(\frac{131}{3}\right)\left(\frac{131}{37}\right)=-\left(\frac{2}{3}\right)\left(\frac{20}{37}\right)$$
$$=\left(\frac{20}{37}\right)=\left(\frac{4\cdot 5}{37}\right)=\left(\frac{5}{37}\right)=\left(\frac{37}{5}\right)=\left(\frac{2}{5}\right)=-1.$$

$$\left(\frac{119}{157}\right)=\left(\frac{7\cdot 17}{157}\right)=\left(\frac{7}{157}\right)\left(\frac{17}{157}\right)=\left(\frac{157}{7}\right)\left(\frac{157}{17}\right)=\left(\frac{3}{7}\right)\left(\frac{4}{17}\right)$$
$$=\left(\frac{3}{7}\right)=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1.$$

$$\left(\frac{365}{1933}\right)=\left(\frac{5\cdot 73}{1933}\right)=\left(\frac{5}{1933}\right)\left(\frac{73}{1933}\right)=\left(\frac{1933}{5}\right)\left(\frac{1933}{73}\right)=\left(\frac{3}{5}\right)\left(\frac{35}{73}\right)$$
$$=\left(\frac{3}{5}\right)\left(\frac{5}{73}\right)\left(\frac{7}{73}\right)=\left(\frac{3}{5}\right)\left(\frac{73}{5}\right)\left(\frac{73}{7}\right)=\left(\frac{3}{5}\right)\left(\frac{3}{5}\right)\left(\frac{3}{7}\right)$$
$$=\left(\frac{3}{7}\right)=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1.$$

11. Vereinfachung der Rechnung durch das Jacobische Symbol.

Wir betrachten das Beispiel (253/257). Was erhalten wir, wenn wir 253 für eine Primzahl halten würden? Wir würden rechnen:

$$\left(\frac{253}{257}\right)=\left(\frac{257}{253}\right)=\left(\frac{4}{253}\right)=1,$$

wie wir auch in Nr. 10 gefunden haben. Oder, wenn wir 111 für eine Primzahl hielten, würden wir rechnen:

$$\left(\frac{111}{131}\right)=-\left(\frac{131}{111}\right)=-\left(\frac{20}{111}\right)=-\left(\frac{4}{111}\right)\left(\frac{5}{111}\right)=-\left(\frac{5}{111}\right)$$
$$=-\left(\frac{111}{5}\right)=-\left(\frac{1}{5}\right)=-1, \text{ wie in Nr. 10.}$$

Oder:

$$\left(\frac{119}{157}\right)=\left(\frac{157}{119}\right)=\left(\frac{38}{119}\right)=\left(\frac{2}{119}\right)\left(\frac{19}{119}\right)=\left(\frac{19}{119}\right)=-\left(\frac{119}{19}\right)$$
$$=-\left(\frac{5}{19}\right)=-\left(\frac{19}{5}\right)=-\left(\frac{4}{5}\right)=-1, \text{ wie in Nr. 10.}$$

Oder:

$$\left(\frac{365}{1933}\right)=\left(\frac{1933}{365}\right)=\left(\frac{108}{365}\right)=\left(\frac{6^2}{365}\right)\left(\frac{3}{365}\right)=\left(\frac{3}{365}\right)=\left(\frac{365}{3}\right)$$

$$=\left(\frac{2}{3}\right)=-1,\text{ wie in Nr. 10. Ist das Zufall?}$$

Wir werden so dazu geführt, das Legendresche Symbol auch für den Fall zu definieren, daß p keine Primzahl ist, und zwar möglichst so, daß die Rechenregeln erhalten bleiben. Nach den Beispielen zu urteilen, erscheint das nicht aussichtslos. Es sei P eine *ungerade* Zahl, und es sei, in Primzahlen zerlegt,

(93) $$P=p_1\,p_2\cdots p_r,$$

wo die p_k Primzahlen sein sollen, die nicht voneinander verschieden zu sein brauchen. Wir definieren dann für ein zu *P teilerfremdes a* das Symbol (a/P) durch die Gleichung

(94) $$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right).$$

Das so definierte Symbol heißt *Jacobisches Symbol.* Wir haben zu untersuchen, ob die im Anfang von Nr. 10 angegebenen Rechenregeln auch für dieses Symbol gelten.

1. Es sei $a\equiv a'$ nach dem Modul P. Das bedeutet, daß $a-a'$ durch P teilbar ist. Dann ist aber $a-a'$ auch durch jedes in P enthaltene p_k teilbar, so daß auch $a\equiv a'$ nach p_k. Daher ist nach Regel 1 in Nr. 10

$$\left(\frac{a}{p_1}\right)=\left(\frac{a'}{p_1}\right),\quad\left(\frac{a}{p_2}\right)=\left(\frac{a'}{p_2}\right),\ \ldots,\ \left(\frac{a}{p_r}\right)=\left(\frac{a'}{p_r}\right)$$

und also nach der Definition (94)

(95) $$\left(\frac{a}{P}\right)=\left(\frac{a'}{P}\right),\ \text{wenn } a\equiv a' \text{ nach } P.$$

2. Ist auch b teilerfremd zu P, so ist nach (94)

(96) $$\left(\frac{b}{P}\right)=\left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_r}\right).$$

Durch Multiplikation von (94) und (96) folgt unter Benutzung der Regel 2, Nr. 10

$$\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)$$

$$=\left(\frac{ab}{p_1}\right)\left(\frac{ab}{p_2}\right)\cdots\left(\frac{ab}{p_r}\right)$$

und in sinngemäßer Anwendung der Definition (94)

(97) $$\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right).$$

Ebenso folgt, wenn auch c teilerfremd ist zu P,

(98) $$\left(\frac{abc}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)\left(\frac{c}{P}\right) \text{ usw.}$$

3. Da nach (94) auch (a/P) nur die Werte $+1$ und -1 haben kann, so folgt aus (98), daß man in a enthaltene quadratische Faktoren fortlassen kann.

4. Da immer $(1/p_k) = 1$, so ist nach (94) auch $(1/P) = 1$.

5. Es sei $a = -1$. *Wir rechnen nach dem Modul 4.* Wir haben dann zwei ungerade Zahlen, -1 und $+1$. Es ist P dann und nur dann gleich -1, wenn von den r Faktoren p_k eine ungerade Anzahl gleich -1 ist. Es ist aber $(-1/p_k)$ dann und nur dann gleich -1, wenn $p_k = -1$ ist. Daher ist nach (94) $(-1/P)$ dann und nur dann gleich -1, wenn eine ungerade Anzahl der Faktoren p_k gleich -1 ist, wenn also $P = -1$ ist. Das heißt aber: Es ist $(-1/P)$ gleich $+1$ oder -1, je nachdem P von der Form $4n+1$ oder $4n-1$ ist.

6. Es sei $a = 2$. *Wir rechnen nach dem Modul 8.* An ungeraden Zahlen haben wir dann $+1$, -1, $+3$, -3. Da

$$\pm 1 \cdot \pm 1 = \pm 1, \quad \pm 1 \cdot \pm 3 = \pm 3, \quad \pm 3 \cdot \pm 3 = \pm 1,$$

so ist P dann und nur dann gleich ± 3, wenn die Anzahl derjenigen Faktoren p_k, die gleich ± 3 sind, ungerade ist. Ferner ist nach Regel 6 in Nr. 10 $(2/p_k)$ dann und nur dann -1, wenn $p_k = \pm 3$. Daher ist wegen (94) $(2/P)$ dann und nur dann gleich -1, wenn die Anzahl der p_k, die gleich ± 3 sind, ungerade ist, wenn also $P = \pm 3$ ist. Das heißt aber: Es ist $(2/P)$ gleich $+1$ oder -1, je nachdem P von der Form $8n \pm 1$ oder $8n \pm 3$ ist.

7. Es sei Q eine *ungerade* zu P *teilerfremde* Zahl, und es sei, in Primzahlen zerlegt,

(99) $$Q = q_1 q_2 \cdots q_s.$$

Es ist dann nach (94) und nach der Rechenregel 2

(100) $$\left(\frac{Q}{P}\right) = \left(\frac{q_1}{p_1}\right)\left(\frac{q_1}{p_2}\right)\cdots\left(\frac{q_s}{p_r}\right).$$

Rechts stehen hier rs Faktoren, da jedes q_k oben und jedes p_k unten steht, in jeder möglichen Zusammensetzung. Wir rechnen nach dem Modul 4, so daß nur die ungeraden Zahlen 1 und -1 vorhanden sind.

Von den Primzahlen p_k mögen α und von den Primzahlen q_k mögen β gleich -1 sein. Es ist P dann und nur dann -1, wenn α, und Q dann und nur dann -1, wenn β ungerade ist. Ferner unterscheiden sich (q_i/p_k) und (p_k/q_i) dann und nur dann durch ein Minuszeichen, wenn p_k und q_i beide gleich -1 sind. In dem Produkt auf der rechten Seite von (100) gibt es genau $\alpha\beta$ Faktoren, wo sowohl die obere wie die untere Zahl gleich -1 ist. Es muß nämlich die untere Zahl gleich einer der α Zahlen p_k sein, die gleich -1 sind, und die obere Zahl gleich einer der β Zahlen q_i, die gleich -1 sind. Diese müssen aber auf alle Arten miteinander kombiniert werden. Nun ist $\alpha\beta$ dann und nur dann ungerade, wenn α und β ungerade sind, wenn also P und Q beide gleich -1 sind. Es unterscheiden sich daher

$$\left(\frac{Q}{P}\right)=\left(\frac{q_1}{p_1}\right)\left(\frac{q_1}{p_2}\right)\cdots\left(\frac{q_s}{p_r}\right) \text{ und } \left(\frac{P}{Q}\right)=\left(\frac{p_1}{q_1}\right)\left(\frac{p_1}{q_2}\right)\cdots\left(\frac{p_r}{q_s}\right)$$

dann und nur dann durch ein Minuszeichen, wenn P und Q beide gleich -1 sind, d. h. die Form $4n-1$ haben. Oder:

Sind P und Q zwei ungerade teilerfremde Zahlen, so ist $(Q/P) = -(P/Q)$, wenn P und Q beide von der Form $4n-1$ sind. Sonst ist $(P/Q) = (Q/P)$.

Wir sehen also, es war kein Zufall. Denn für das neue Jacobische Symbol (a/P), wo P eine ungerade zu a teilerfremde Zahl ist, gelten genau dieselben Rechenregeln wie für das ursprüngliche Legendresche Symbol. Aber bitte, lieber Leser, komme nicht auf den Gedanken, es hätte auch dieselbe *Bedeutung*. Es ist *nicht* so, daß (a/P) dann und nur dann gleich $+1$ ist, wenn a quadratischer Rest von P ist, wenn es also eine Quadratzahl gibt, die sich von a nur durch ein Vielfaches von P unterscheidet. Es ist zum Beispiel $(a/25) = (a/5)^2 = +1$ für beliebiges zu 5 teilerfremdes a. Es ist aber sicher nicht jedes solche a quadratischer Rest von 25.

Beispiele:

$$\left(\frac{1007}{1933}\right)=\left(\frac{1933}{1007}\right)=\left(\frac{-81}{1007}\right)=\left(\frac{-1}{1007}\right)\left(\frac{9^2}{1007}\right)=-1.$$

Oder auf die frühere Art:

$$\left(\frac{1007}{1933}\right)=\left(\frac{19}{1933}\right)\left(\frac{53}{1933}\right)=\left(\frac{1933}{19}\right)\left(\frac{1933}{53}\right)=\left(\frac{-5}{19}\right)\left(\frac{25}{53}\right)$$

$$=\left(\frac{-1}{19}\right)\left(\frac{5}{19}\right)=-\left(\frac{5}{19}\right)=-\left(\frac{19}{5}\right)=-\left(\frac{4}{5}\right)=-1.$$

$$\left(\frac{525}{1009}\right)=\left(\frac{1009}{525}\right)=\left(\frac{484}{525}\right)=\left(\frac{22^2}{525}\right)=1.$$

Oder:

$$\left(\frac{525}{1009}\right) = \left(\frac{21 \cdot 5^2}{1009}\right) = \left(\frac{3}{1009}\right)\left(\frac{7}{1009}\right) = \left(\frac{1009}{3}\right)\left(\frac{1009}{7}\right)$$
$$= \left(\frac{1}{3}\right)\left(\frac{1}{7}\right) = 1.$$

Wir haben also einen Weg, auf dem wir bestimmen können, ob eine Zahl a QR einer Primzahl p ist oder nicht, ob also $\sqrt{a}$ nach dem Modul p vorhanden ist oder nicht. Ist $(a/p) = +1$, so haben wir zur *Bestimmung* von $\sqrt{a}$ nur die Möglichkeit, die Quadrate der Zahlen von 1 bis $\frac{1}{2}(p-1)$ zu berechnen und zu sehen, welches von ihnen nach p gleich a ist. Man vergleiche hierzu Nr. 7 in Abschnitt VIII.

12. Zwei Aufgaben.

1. Von welchen ungeraden Primzahlen p ist 5 QR?

Da 5 die Form $4n+1$ hat, so ist 5 QR von p, wenn p QR von 5 ist, wenn also p nach dem Modul 5 gleich ± 1 ist. Wir haben daher:

Es ist 5 QR aller Primzahlen der Form $5n \pm 1$ und QN aller von der Form $5n \pm 2$.

2. Von welchen ungeraden Primzahlen p ist 3 QR?

Wir haben jetzt zwei Fälle zu unterscheiden, je nachdem p von der Form $4n+1$ oder $4n-1$ ist.

Fall 1: Es ist p von der Form $4n+1$. Es ist 3 QR von p, wenn p QR von 3 ist, wenn also p nach dem Modul 3 gleich 1 ist. Es muß daher p sowohl bei der Teilung durch 4 wie bei der durch 3 den Rest 1 lassen, so daß $p-1$ durch 3 und 4, also durch 12 teilbar ist.

Fall 2: Es ist p von der Form $4n-1$. Dann ist 3 QR von p, wenn p QN von 3 ist, wenn also p die Form $3n-1$ hat. Es muß daher $p+1$ durch 3 und durch 4 teilbar sein, also durch 12. Ergebnis:

Es ist 3 QR aller Primzahlen der Form $12n \pm 1$ und QN aller von der Form $12n \pm 5$.

Bemerkung: Die ungeraden Zahlen der Form $12n \pm 3$ sind, abgesehen von 3, keine Primzahlen.

13. Quadratische Reste von der Potenz einer ungeraden Primzahl.

Es sei p eine Primzahl und α eine positive Zahl. Dann heißt eine nicht durch p teilbare Zahl a ein QR von p^α, wenn sie nach dem Modul p^α gleich einer Quadratzahl ist, sonst QN von p^α. Die durch p teilbaren

Zahlen lassen wir also beiseite. In dieser Nummer betrachten wir den Fall, wo p *ungerade* ist. Dann gilt:

Eine Zahl a ist dann und nur dann QR von der Potenz einer ungeraden Primzahl p, wenn sie QR von p ist.

Der erste Teil der Behauptung ist klar. Denn wenn a nach dem Modul p^α gleich einer Quadratzahl g^2 ist, so ist sie auch nach dem Modul p gleich einer Quadratzahl, nämlich auch gleich g^2. Den zweiten Teil der Behauptung werden wir dadurch beweisen, daß wir zeigen, wie man immer eine Zahl x_k finden kann, so daß $x_k^2 - a$ durch p^k teilbar ist, sobald man eine Zahl x_1 kennt, für die $x_1^2 - a$ durch p teilbar ist.

Es sei $(a/p) = 1$, und x_1 sei einer der Werte von $\sqrt{a}$, so daß $x_1^2 - a$ durch p teilbar ist. Unser Ziel ist, der Reihe nach Zahlen x_2, x_3 usw. so zu bestimmen, daß $x_2^2 - a$ durch p^2, $x_3^2 - a$ durch p^3 teilbar wird, usw. Bei x_1 kommt es auf Vielfache von p nicht an. Setzen wir daher $x_2 = x_1 + y_1 p$, so ist $x_2^2 - a$ jedenfalls durch p teilbar, und wir können versuchen, die Zahl y_1 so zu bestimmen, daß $x_2^2 - a$ durch p^2 teilbar wird, also nach dem Modul p^2 gleich 0 ist. Nach dem Modul p^2 ist aber, wenn wir $x_1^2 - a = a_1 p$ setzen,

$$x_2^2 - a = (a_1 + 2\,x_1 y_1)p,$$

und das ist dann und nur dann 0 nach p^2, wenn $a_1 + 2\,x_1 y_1 = 0$ nach p. Da $x_1 = \sqrt{a}$ nicht durch p teilbar ist, und da p ungerade ist, so ist $2x_1$ zu p teilerfremd, und daher ergibt sich y_1 eindeutig gleich $-a_1/2x_1$ nach p. Wir bezeichnen den Wert, den $-1/2x_1$ nach dem Modul p hat, mit z, so daß $y_1 = a_1 z$ wird. Es ist aber zu beachten, daß y_1 nur bis auf Vielfache von p bestimmt ist. Wir werden immer für y_1 den positiv kleinsten Rest nach p wählen, um nicht unnötig große Zahlen zu erhalten. Es ist jetzt $x_2^2 - a$ durch p^2 teilbar, und wir setzen $x_2^2 - a = a_2 p^2$. Setzen wir $x_3 = x_2 + y_2 p^2$, so ist auch $x_3^2 - a$ durch p^2 teilbar, und wir bestimmen y_2 so, daß $x_3^2 - a$ den Teiler p^3 bekommt. Nach dem Modul p^3 ist

$$x_3^2 - a = (a_2 + 2\,x_2 y_2)p^2,$$

und das ist dann und nur dann 0 nach p^3, wenn $a_2 + 2\,x_2 y_2 = 0$ nach p. Da aber $x_2 = x_1$ nach p, so ergibt sich eindeutig $y_2 = -a_2/2x_1 = a_2 z$. Dabei ist wieder daran zu denken, daß es bei y_2 wie bei y_1 auf Vielfache von p nicht ankommt. Wir setzen $x_3^2 - a = a_3 p^3$, wo a_3 ganz ist. Ferner wählen wir $x_4 = x_3 + y_3 p^3$ und bestimmen y_3 aus der Bedingung, daß $x_4^2 - a$ durch p^4 teilbar sein soll. Wir finden $y_3 = a_3 z$ nach p. In dieser Weise können wir fortfahren, bis wir zu einer Zahl x_α kommen mit der Eigenschaft, daß $x_\alpha^2 - a$ durch die gegebene Potenz p^α von p teilbar ist. Wir stellen die zur Berechnung dienenden Formeln übersichtlich zusammen.

$$x_1 = \sqrt{a}, \quad -1/2x_1 = z \text{ nach } p.$$

$(x_1^2 - a)/p = a_1$, $y_1 = a_1 z$ nach p, $x_2 = x_1 + y_1 p$;
$(x_2^2 - a)/p^2 = a_2$, $y_2 = a_2 z$ nach p, $x_3 = x_2 + y_2 p^2$;
$(x_3^2 - a)/p^3 = a_3$, $y_3 = a_3 z$ nach p, $x_4 = x_3 + y_3 p^3$; usw.

Das Verfahren sei an einigen Beispielen erläutert.

Beispiel 1: $p = 7$, $p^2 = 49$, $p^3 = 343$, $p^4 = 2401$; $a = 86$, $\alpha = 4$.
Es ist $(86/7) = (2/7) = 1$, $x_1 = 3$, $z = -1/6 = 6/6 = 1$.

$(3^2 - 86)/7 = -11 = a_1$, $y_1 = -11 = 3$, $x_2 = 3 + 3 \cdot 7 = 24$;
$(24^2 - 86)/49 = (576 - 86)/49 = 10 = a_2, y_2 = 10 = 3$,
$x_3 = 24 + 3 \cdot 49 = 171$;
$(171^2 - 86)/343 = (29241 - 86)/343 = 85 = a_3, y_3 = 85 = 1$,
$x_4 = 171 + 1 \cdot 343 = 514$.

Es ist daher $514^2 - 86$ durch 7^4 teilbar, oder es ist ein Wert von $\sqrt{86}$ nach dem Modul 7^4 gleich 514.

Beispiel 2: $p = 5$, $p^2 = 25$, $p^3 = 125$, $p^4 = 625$, $p^5 = 3125$; $a = 101$.
Es ist $(101/5) = (1/5) = 1$, $x_1 = 1$, $z = -1/2 = 4/2 = 2$.

$(1^2 - 101)/5 = -20 = a_1, y_1 = -40 = 0, x_2 = x_1 = 1$;
$(1^2 - 101)/25 = -4 = a_2$, $y_2 = -8 = 2$, $x_3 = 1 + 2 \cdot 25 = 51$,
$(51^2 - 101)/125 = (2601 - 101)/125 = 20 = a_3$, $y_3 = 40 = 0$,
$x_4 = x_3 = 51$,
$(51^2 - 101)/625 = 4 = a_4$, $y_4 = 8 = 3$, $x_5 = 51 + 3 \cdot 625 = 1926$.

Es ist daher nach dem Modul $5^5 = 3125$ ein Wert von $\sqrt{101}$ gleich 1926.

Beispiel 3: $p = 17$, $p^2 = 289$, $p^3 = 4913$, $p^4 = 83521$; $a = 3408$.
Es ist $(3408/17) = (8/17) = (2/17) = 1$, $x_1 = 5$, $z = -1/10 = -120/10 = -12 = 5$.

$(5^2 - 3408)/17 = -199 = a_1, y_1 = -5 \cdot 199 = -5 \cdot 12 = -60 = 8$,
$x_2 = 5 + 8 \cdot 17 = 141$;
$(141^2 - 3408)/289 = 16473/289 = 57 = a_2$, $y_2 = 5 \cdot 57 = 5 \cdot 6 = 30 = 13$;
$x_3 = 141 + 13 \cdot 289 = 3898$;
$(3898^2 - 3408)/4913 = 15190996/4913 = 3092 = a_3$,
$y_3 = 5 \cdot 3092 = 5 \cdot -2 = 7, x_4 = 3898 + 7 \cdot 4913 = 38289$.

Daher ist einer der Werte von $\sqrt{3408}$ nach dem Modul 17^4 gleich 38289.

Wir sehen: Ist a QR von p und kennen wir einen der beiden Werte, die $\sqrt{a}$ nach dem Modul p hat, so können wir eine Zahl g so bestimmen, daß $g^2 - a$ durch eine gegebene Potenz von p teilbar wird. Dabei ist nur *eine* Divisionsaufgabe zu lösen, nämlich die Bestimmung von $z = -1/2x_1$. Im übrigen verwenden wir nur Addition, Subtraktion und Multiplikation. Wir erhalten so einen der Werte, etwa g, die $\sqrt{a}$ nach

dem Modul p^α hat. Es fragt sich, ob $\sqrt{a}$ noch andere Werte haben kann und welche. Es sei außer g^2 auch h^2 nach p^α gleich a. Dazu ist notwendig und hinreichend, daß

$$g^2 - h^2 = (g - h)\ (g + h)$$

durch p^α teilbar ist. Es können nicht beide Faktoren $g - h$ und $g + h$ den Teiler p haben, weil ihn sonst auch ihre Summe $2g$ hätte. Daher ist der eine der Faktoren zu p teilerfremd und der andere durch p^α teilbar. Es ist also entweder $h = g$ oder $h = -g$ nach p^α. Ergebnis:

Ist p eine ungerade Primzahl und α eine positive Zahl, so ist $\sqrt{a}$ nach dem Modul p^α dann und nur dann vorhanden, wenn a QR von p ist. Es hat dann $\sqrt{a}$ zwei Werte, die sich nur durch das Vorzeichen unterscheiden.

14. Quadratische Reste einer Potenz von 2.

Wir beschränken uns auf zu 2 teilerfremde, also ungerade Zahlen.

Nach dem Modul 2 gibt es nur eine ungerade Zahl, die 1, und diese ist QR von 2. Daher ist jede ungerade Zahl a QR von 2, und es hat $\sqrt{a}$ nach 2 nur den einen Wert 1.

Nach dem Modul 4 gibt es zwei ungerade Zahlen, 1 und $3 = -1$. Ihre Quadrate sind beide gleich 1. Es sind daher die Zahlen der Form $4n + 1$ und nur diese QR von 4, und wenn a eine solche Zahl ist, so hat $\sqrt{a}$ nach 4 die beiden Werte ± 1.

Nach dem Modul 8 gibt es vier ungerade Zahlen, 1, 3, 5, 7 oder ± 1, ± 3. Ihre Quadrate sind gleich 1, so daß eine Zahl a dann und nur dann QR von 8 ist, wenn sie die Form $8n + 1$ hat, und $\sqrt{a}$ hat die vier Werte ± 1, ± 3 nach dem Modul 8.

Es sei jetzt α eine Zahl, die mindestens gleich 3 ist. Soll eine ungerade Zahl a QR von 2^α sein, so muß sie jedenfalls QR von $2^3 = 8$ sein, also die Form $8n + 1$ haben. Wir zeigen, daß diese Bedingung auch hinreicht, und zwar, indem wir ähnlich wie in der vorigen Nummer der Reihe nach Zahlen x_1, x_2, x_3 usw. bestimmen, so daß $x_k^2 - a$ durch 2^k teilbar wird. Wir wählen $x_1 = x_2 = x_3 = 1$. Da a von der Form $8n + 1$ sein muß, so wird $1^2 - a$ durch 8 teilbar. Wir setzen $1^2 - a = 8a_3$. Wählen wir $x_4 = x_3 + 4y_3$, so wird $x_4^2 - a = 8(a_3 + x_3 y_3)$ nach dem Modul 2^4. Es wird daher $x_4^2 - a$ durch 16 teilbar, wenn $a_3 + x_3 y_3$ eine gerade Zahl ist. Da $x_3 = 1$, so ist das der Fall, wenn $y_3 = -a_3 = a_3$ nach 2. Wir wählen also y_3 gleich 0 oder 1, je nachdem a_3 gerade oder ungerade ist. Wir setzen $x_4^2 - a = 2^4 a_4$ und $x_5 = x_4 + 2^3 y_4$. Es wird $x_5^2 - a = 2^4(a_4 + x_4 y_4)$ nach dem Modul 2^5, so daß $x_5^2 - a$ durch 2^5 teilbar wird, wenn $a_4 + x_4 y_4$ gerade ist. Da $x_4 = x_3 + 4y_3 = 1 + 4y_3$, so ist x_4 ungerade, und y_4 muß nach 2 gleich a_4 sein. Wir setzen dann $x_5^2 - a = 2^5 a_6$

und $x_6 = x_5 + 2^4 y_5$, wo wir y_5 gleich 0 oder 1 wählen, je nachdem a_5 gerade oder ungerade ist. In dieser Weise können wir fortfahren, bis wir zu der gesuchten Zahl x_α kommen. Wir stellen die Formeln übersichtlich zusammen.

Es sei a eine Zahl der Form $8n + 1$. Wir setzen $x_3 = 1$ und dann rechnen wir nach dem Schema:

$(x_3^2 - a)/8 = a_3$, $y_3 = a_3$ nach 2, $x_4 = x_3 + 2^2 y_3$;
$(x_4^2 - a)/16 = a_4$, $y_4 = a_4$ nach 2, $x_5 = x_4 + 2^3 y_4$;
$(x_5^2 - a)/32 = a_5$, $y_5 = a_5$ nach 2, $x_6 = x_5 + 2^4 y_5$; usw.

Es ist dann $x_\alpha^2 - a$ durch 2^α teilbar. Es sei noch darauf hingewiesen, daß y_k gleich 0 oder 1 ist, je nachdem a_k gerade oder ungerade ist.

Beispiel: $a = 1001 = 8 \cdot 125 + 1$; $x_3 = 1$, $\alpha = 11$.
$(1^2 - 1001)/8 = -125 = a_3$, $y_3 = 1$, $x_4 = 1 + 4 = 5$;
$(5^2 - 1001)/16 = -61 = a_4$, $y_4 = 1$, $x_5 = 5 + 8 = 13$;
$(13^2 - 1001)/32 = -26 = a_5$, $y_5 = 0$, $x_6 = x_5 = 13$;
$(13^2 - 1001)/64 = -13 = a_6$, $y_6 = 1$, $x_7 = 13 + 32 = 45$;
$(45^2 - 1001)/128 = 8 = a_7$, $y_7 = 0$, $x_8 = x_7 = 45$;
$a_8 = 4$, $y_8 = 0$, $x_9 = x_8$; $a_9 = 2$, $y_9 = 0$, $x_{10} = x_9 = 45$;
$a_{10} = 1$, $y_{10} = 1$, $x_{11} = 45 + 2^9 = 45 + 512 = 557$.

Es ist daher $557^2 - 1001$ durch $2^{11} = 2048$ teilbar. Es ist in der Tat $557^2 - 1001 = 310249 - 1001 = 309248 = 151 \cdot 2048$.

Nachdem wir gesehen haben, wie wir immer einen der Werte, die $\sqrt{a}$ nach dem Modul 2^α hat, finden können, fragen wir nach den etwa vorhandenen anderen Werten. Es sei g der gefundene Wert und h ein anderer. Dann ist

$$g^2 - h^2 = (g - h)(g + h)$$

durch 2^α teilbar, und, wenn das der Fall ist, so ist gleichzeitig mit g auch h ein Wert von $\sqrt{a}$. Da g und h ungerade Zahlen sind, so sind beide Faktoren $g - h$ und $g + h$ durch 2 teilbar, aber nicht beide durch 4. Denn ihre Summe, $2g$, ist nicht durch 4 teilbar. Daher muß einer der Faktoren mindestens durch $2^{\alpha-1}$ teilbar sein. Nach dem Modul 2^α muß daher h gleich g, $g + 2^{\alpha-1}$, $-g$ oder $-g - 2^{\alpha-1}$ sein. Es hat zum Beispiel $\sqrt{1001}$ nach dem Modul 2048 die 4 Werte ± 557, ± 1581 oder auch die Werte 557, $2048 - 557 = 1491$, 1581, $2048 - 1581 = 467$.

Ergebnis:

Nach dem Modul 2 ist $\sqrt{a}$ für jede ungerade Zahl a vorhanden und hat den Wert 1.

Nach dem Modul 4 ist $\sqrt{a}$ für jede Zahl der Form $4n + 1$ vorhanden und hat die Werte ± 1.

Für $\alpha \geqq 3$ ist $\sqrt{a}$ für jedes a der Form $8n+1$ nach dem Modul 2^α vorhanden und hat vier Werte. Ist g einer von ihnen, so sind die anderen $-g$, $g+2^{\alpha-1}$, $-(g+2^{\alpha-1})$.

15. Quadratische Reste von einer ganzen Zahl *m*.

Es sei m eine positive Zahl und a irgendeine Zahl. Wir stellen uns folgende drei Fragen:

1. Wann gibt es eine Zahl x, so daß $x^2 - a = 0$ nach dem Modul m, wann ist also $\sqrt{a}$ nach dem Modul m vorhanden?

2. Wie finden wir die etwa vorhandenen Werte von $\sqrt{a}$?

3. Wie viele nach dem Modul m verschiedene Werte von $\sqrt{a}$ gibt es, wenn es überhaupt welche gibt?

Wir beschränken uns in dieser Nummer auf den Fall, wo a und m teilerfremd sind. *In diesem Falle heißt a ein QR von m, wenn die Gleichung $x^2 - a = 0$ nach m eine Lösung hat.* Wir schreiben m in der Form

$$(101) \qquad m = 2^\mu p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

wo die p_k voneinander verschiedene ungerade Primzahlen sein sollen. Ist $x^2 - a$ durch m teilbar, so auch durch jeden Teiler von m. Es ist daher a QR eines jeden Teilers von m, wenn es QR von m ist. Notwendig dafür, daß a QR von m ist, ist also, daß erstens a QR von jeder in m enthaltenen ungeraden Primzahl ist, und daß zweitens a QR von 2, 4 oder 8 ist, wenn $\mu = 1$, 2 oder größer als 2 ist. Diese Bedingungen seien erfüllt. Wir bestimmen dann r Zahlen $x_1, x_2, \ldots, x_r$ so, daß

$$(102) \qquad x_k^2 - a = 0 \text{ nach } p_k^{\alpha_k}.$$

Nach Nr. 13 ist das möglich. Ist $\mu > 0$, so bestimmen wir ferner eine Zahl x_0 so, daß

$$(103) \qquad x_0^2 - a = 0 \text{ nach } 2^\mu,$$

was nach Nr. 14 ausführbar ist. Dann berechnen wir eine Zahl x, die nach dem Modul $p_k^{\alpha_k}$ gleich x_k ist, und zwar für $k = 1, 2, \ldots, r$, und die ferner, wenn $\mu > 0$, nach dem Modul 2^μ gleich x_0 ist. Man vergleiche Abschnitt V, Nr. 6. Wir können uns diese Zahl x in folgender Weise herstellen. Zunächst setzen wir

$$(104) \qquad m_0 = \frac{m}{2^\mu}, \quad m_k = \frac{m}{p_k^{\alpha_k}}.$$

Es ist m_k teilerfremd zu $p_k^{\alpha_k}$, so daß die Zahl $1/m_k$ nach dem Modul $p_k^{\alpha_k}$

vorhanden ist. Das heißt, es gibt eine Zahl y_k, so daß

(105) $$y_k m_k \equiv 1 \text{ nach } p_k^{\alpha_k}.$$

Ist $\mu > 0$, so gibt es, da m_0 ungerade ist, eine Zahl y_0, so daß

(106) $$y_0 m_0 \equiv 1 \text{ nach } 2^\mu.$$

Ist $\mu = 0$, so setzen wir

(107) $$x = x_1 y_1 m_1 + x_2 y_2 m_2 + \cdots + x_r y_r m_r,$$

und, wenn $\mu > 0$, so sei

(108) $$x = x_0 y_0 m_0 + x_1 y_1 m_1 + \cdots + x_r y_r m_r.$$

Rechnen wir nach dem Modul $p_k^{\alpha_k}$, so sind die Zahlen m_i alle 0 bis auf m_k und nach (105) ist $y_k m_k \equiv 1$. Daher wird nach (107) und (108) $x \equiv x_k$, wie wir es wünschten. Ist $\mu > 0$, so sind alle m_i, außer m_0, durch 2^μ teilbar, also gleich 0 nach dem Modul 2^μ, während $y_0 m_0$ nach 2^μ gleich 1 ist. Rechnen wir daher nach dem Modul 2^μ, so werden alle m_i zu 0, außer m_0, und nach (106) wird $y_0 m_0$ gleich 1. Daher wird nach (108) $x \equiv x_0$, wie wir es haben wollten.

Es ist also unter Benutzung von (102)

$$x \equiv x_k, \quad x^2 - a \equiv x_k^2 - a \equiv 0 \text{ nach } p_k^{\alpha_k}.$$

Ferner ist für $\mu > 0$ wegen (106)

$$x \equiv x_0, \quad x^2 - a \equiv x_0^2 - a \equiv 0 \text{ nach } 2^\mu.$$

Daher ist $x^2 - a$ durch 2^μ, durch $p_1^{\alpha_1}$, durch $p_2^{\alpha_2}, \ldots$, durch $p_r^{\alpha_r}$ teilbar, also auch durch m, d. h. es ist

(109) $$x^2 - a \equiv 0 \text{ nach } m.$$

Damit haben wir gezeigt, daß und wie wir eine Lösung von (109) finden können. Die oben angegebenen notwendigen Bedingungen dafür, daß a ein QR von m ist, sind also auch hinreichend. Daher haben wir:

Es sei m eine positive Zahl. Sie enthalte den Faktor 2 in der μ-ten Potenz. Ferner sei a eine zu m teilerfremde Zahl. Dann ist a dann und nur dann QR von m, wenn a QR von jeder in m aufgehenden ungeraden Primzahl ist, und wenn a für $\mu = 2$ QR von 4 und für $\mu > 2$ QR von 8 ist.

Wir fragen uns jetzt, wie wir aus einem Werte von $\sqrt{a}$ nach dem Modul m die etwa vorhandenen anderen finden können. Dabei wird sich dann auch ergeben, wie viele Werte $\sqrt{a}$ hat. Es sei g einer der Werte von $\sqrt{a}$. Irgendein anderer sei h. Es ist sowohl g^2 wie h^2 nach m gleich a, so daß

(110) $$g^2 - h^2 = (g - h)(g + h)$$

durch m teilbar sein muß. Ist das der Fall, so ist umgekehrt mit g auch h ein Wert von $\sqrt{a}$. Wir setzen

$$(111) \qquad m = 2^{\mu} m_0, \quad m_0 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

wo, wie in (101), die p_k voneinander verschiedene ungerade Primzahlen sind. Da a teilerfremd zu m ist, so gilt dasselbe von g und h. Für $\mu > 0$ sind daher g und h ungerade. Wir unterscheiden verschiedene Fälle.

Fall 1. Es sei $\mu = 0$.

Es ist $m = m_0$ eine ungerade Zahl, also nicht nur zu g, sondern auch zu $2g$ teilerfremd. Daher können die Faktoren $g - h$ und $g + h$ keinen gemeinsamen Teiler haben, der in m aufgeht. Denn der würde auch in ihrer Summe, $2g$, enthalten sein. Nun muß sich m in zwei Faktoren s und t so zerlegen lassen, daß der eine ein Teiler von $g - h$, der andere von $g + h$ ist, damit $g^2 - h^2$ durch m teilbar wird. Nach dem eben Gesagten müssen s und t teilerfremd sein. Es seien jetzt

$$(112) \qquad s_1 t_1, \; s_2 t_2, \ldots, s_\rho t_\rho$$

die sämtlichen Zerlegungen von $m = m_0$ in je zwei zueinander teilerfremde Faktoren. Dabei sollen zwei Zerlegungen auch dann als verschieden gelten, wenn sie sich nur durch die Reihenfolge der Faktoren unterscheiden. Soll $g^2 - h^2$ durch m_0 teilbar werden, so kann das nur auf eine der ρ Arten geschehen, daß $g - h$ durch s_k und $g + h$ durch t_k teilbar wird. Wir haben also zu versuchen, ρ Zahlen $h_1, h_2, \ldots, h_\rho$ so zu bestimmen, daß

$$(113) \qquad h_k = \begin{cases} \;\; g \text{ nach } s_k, \\ -g \text{ nach } t_k. \end{cases}$$

Nach Abschnitt V, Nr. 6 ist hierdurch h_k nach dem Modul $s_k t_k = m$ eindeutig bestimmt, da $(s_k, t_k) = 1$. Daher gibt es nach m genau ρ Werte für $\sqrt{a}$, nämlich die Werte $h_1, h_2, \ldots, h_\rho$. Unter diesen ist natürlich g enthalten. Es ist etwa $h_\rho = g$, wenn $s_\rho = m$, $t_\rho = 1$ ist.

Frage: In welcher Beziehung stehen zwei Werte von $\sqrt{a}$, die zwei Zerlegungen von m entsprechen, die sich nur durch die Reihenfolge der Faktoren unterscheiden?

Wir haben noch die Anzahl ρ der möglichen Zerlegungen von m in je zwei teilerfremde Faktoren zu bestimmen. Jede Zerlegung ist durch die Angabe des ersten Faktors vollständig bestimmt. Enthält ferner s_i eine der Primzahlen p_k, so muß s_i sie in derselben Potenz enthalten wie m, da ja sonst t_i nicht teilerfremd zu s_i wäre. Daher ist s_i vollkommen bestimmt durch die Angabe derjenigen der r Primzahlen p_k, die in s_i vorkommen. Es gibt zum Beispiel ein s_i, das kein p_k enthält; es ist gleich 1.

Es gibt r Zahlen s_i, die je ein p_k enthalten. Um ein bestimmtes s_i zu kennzeichnen, schreiben wir die r Primzahlen p_k senkrecht untereinander und rechts neben jedes p_k ein $+$ oder $-$ Zeichen, je nachdem es in s_i aufgenommen werden soll oder nicht. Wir erhalten daher alle s_i und jedes nur einmal, indem wir die Zeichen $+$ und $-$ auf alle möglichen Arten auf die r Felder einer Spalte verteilen. Schreiben wir diese Spalten nebeneinander, so erhalten wir eine Tabelle für die verschiedenen s_i. Für die kleinsten Werte von r erhalten wir:

$r = 1.$

p_1	+	—

$r = 2.$

p_1	+	—	+	—
p_2	+	+	—	—

$r = 3.$

p_1	+	—	+	—	+	—	+	—
p_2	+	+	—	—	+	+	—	—
p_3	+	+	+	+	—	—	—	—

$r = 4.$

p_1	+	—	+	—	+	—	+	—	+	—	+	—	+	—	+	—
p_2	+	+	—	—	+	+	—	—	+	+	—	—	+	+	—	—
p_3	+	+	+	+	—	—	—	—	+	+	+	+	—	—	—	—
p_4	+	+	+	+	+	+	+	+	—	—	—	—	—	—	—	—

Es bedeutet zum Beispiel die zweite Spalte der Tabelle für $r = 3$ dasjenige s_i, in das p_2 und p_3 aufgenommen sind. Jede der Tabellen enthält eine Zeile mehr als die vorhergehende, und wir können das in jeder Spalte neu hinzukommende Feld mit dem Zeichen $+$ oder $-$ ausfüllen. Daher erhalten wir jede Tabelle aus der vorhergehenden, indem wir diese zweimal nebeneinander schreiben, wobei wir das eine Mal jeder Spalte das Zeichen $+$ und das andere Mal das Zeichen $-$ anfügen. Es hat also jede Tabelle doppelt so viel Spalten wie die vorhergehende. Da die erste 2 Spalten hat, so hat die zweite $2 \cdot 2 = 2^2$, die dritte $2 \cdot 2^2 = 2^3$, und die r-te 2^r Spalten. Das heißt aber: Die Anzahl der möglichen s_i oder die gesuchte Zahl ρ ist gleich 2^r.

Wir haben also

(114) $$\rho = 2^r.$$

Fall 2. $\mu = 1$ *oder* 2.

Da in diesem Falle g und h ungerade sind, so sind $g - h$ und $g + h$ beide durch 2 teilbar und $g^2 - h^2$ ist ganz von selbst durch 4 teilbar. Wir müssen aber dafür sorgen, daß h ungerade ist. Die Zahl g ist als einer der Werte von $\sqrt{a}$ sicher ungerade. Zunächst muß wieder $g^2 - h^2$ durch m_0 teilbar sein. Wir bestimmen also wieder die ρ Zahlen h_k aus (113). Diese sind eindeutig bestimmt bis auf Vielfache von m_0. Es ist aber diesmal nicht $m_0 = m$, so daß zwei Zahlen nach m_0 gleich sein

können, ohne es nach m zu sein. Mit h_k sind auch die Zahlen

(115) $$h_k,\ h_k \pm m_0,\ h_k \pm 2m_0,\ h_k \pm 3m_0, \ldots$$

Lösungen von (113). Es fragt sich, wie viele von diesen nach m verschieden sind. Dabei ist weiter zu beachten, daß h_k ungerade sein muß. Da m_0 ungerade ist, so ist von den beiden Zahlen h_k und $h_k + m_0$ die eine gerade und die andere ungerade, so daß die Gleichungen (113) immer eine ungerade Lösung haben. Wir nehmen an, daß h_k eine solche ist. Dann sind auch die Zahlen

(116) $$h_k,\ h_k \pm 2m_0,\ h_k \pm 4m_0, \ldots$$

ungerade Lösungen von (113). Ist $\mu = 1$, so ist $2m_0 = m$, und die Zahlen (116) sind nach dem Modul m einander gleich, so daß h_k durch (113) eindeutig nach dem Modul m bestimmt ist. Es hat also $\sqrt{a}$ nach dem Modul m wieder $\rho = 2^r$ verschiedene Werte. Ist $\mu = 2$, so ist $4m_0 = m$, und von den Zahlen (116) sind zwei nach m verschieden, etwa h_k und $h_k + 2m_0$. Wir erhalten daher für $\sqrt{a}$ nach dem Modul m jetzt $2\rho = 2^{r+1}$ verschiedene Werte, nämlich die ρ Zahlen h_k und die ρ Zahlen $h_k + 2m_0$.

Fall 3. Es sei $\mu \geq 3$.

Es sind g und h wieder ungerade, so daß die Faktoren $g - h$ und $g + h$ wieder beide durch 2 teilbar sind; sie sind aber nicht beide durch 4 teilbar, weil ihre Summe $2g$ es nicht ist. Daher muß der eine der beiden Faktoren durch $2^{\mu-1}$ teilbar sein. Dieser ist dann wegen $\mu \geq 3$ gewiß eine gerade Zahl, so daß h von selbst ungerade wird, da g als einer der Werte von $\sqrt{a}$ sicher ungerade ist. Ist daher der eine der Faktoren $g - h$ und $g + h$ durch $2^{\mu-1}$ teilbar, so ist der andere immer durch 2 teilbar, so daß das Produkt durch 2^μ teilbar wird. Wir setzen

$$s'_k = 2^{\mu-1} s_k, \quad t'_k = 2^{\mu-1} t_k.$$

Wir haben dann für $2^{\mu-1} m_0$ die 2ρ Zerlegungen in je zwei teilerfremde Faktoren

$$s'_1 t_1,\ s'_2 t_2,\ \ldots,\ s'_\rho t_\rho,$$
$$s_1 t'_1,\ s_2 t'_2,\ \ldots,\ s_\rho t'_\rho.$$

Soll $(g - h)(g + h)$ durch $m = 2^\mu m_0$ teilbar werden, so ist dazu nach den angestellten Betrachtungen notwendig und hinreichend, daß entweder der erste der Faktoren durch ein s'_k, der zweite dann durch t_k teilbar ist, oder daß der erste durch s_k, der zweite durch t'_k teilbar ist. Die möglichen Werte für h sind also die Lösungen der Gleichungen

(117) $$h'_k = \begin{cases} g \text{ nach } s'_k, \\ -g \text{ nach } t_k, \end{cases} \qquad h''_k = \begin{cases} g \text{ nach } s_k, \\ -g \text{ nach } t'_k. \end{cases}$$

Da $(s'_k, t_k) = (s_k, t'_k) = 1$, so haben diese Gleichungspaare je eine Lösung nach dem Modul $s'_k t_k = s_k t'_k = 2^{\mu-1} m_0$. Wir erhalten weitere durch Addition von Vielfachen von $2^{\mu-1} m_0$. Da aber schon das Zweifache dieser Zahl gleich m ist, so sind nur die vier Zahlen

$$h'_k,\ h'_k + 2^{\mu-1} m_0,\ h''_k,\ h''_k + 2^{\mu-1} m_0$$

nach dem Modul m verschieden. Da k jeden der Werte von 1 bis ρ annehmen kann, so erhalten wir für h, das heißt für $\sqrt{a}$ im ganzen $4\rho = 2^{r+2}$ verschiedene Werte. Ergebnis:

Es sei m eine positive Zahl und a eine zu m teilerfremde Zahl. Ferner sei a QR von m. Es habe m die Form $2^\mu m_0$, wo die ungerade Zahl m_0 r verschiedene Primzahlen enthalte. Dann hat $\sqrt{a}$ nach dem Modul m

2^r Werte, wenn $\mu = 0$ oder 1,
2^{r+1} Werte, wenn $\mu = 2$,
2^{r+2} Werte, wenn $\mu \geq 3$.

16. Die Wurzel aus a nach einem Modul m.

Wir wollen in dieser Nummer die drei Fragen beantworten, die wir im Anfang der vorigen Nummer gestellt haben, aber ohne die Einschränkung, daß a und m teilerfremd sein sollen. Die Fragen beziehen sich auf die Auflösung der Gleichung

(118) $$x^2 - a = 0 \text{ nach dem Modul } m.$$

Den g. g. T. d von a und m schreiben wir in der Form

(119) $$d = (a, m) = g^2 h,$$

wo h die in ungerader Potenz in d aufgehenden Primzahlen enthalten soll, und zwar jede in der ersten Potenz. Es ist dann g eine ganze Zahl. Aus (118) folgt, daß x^2 durch $d = g^2 h$, also x durch gh teilbar sein muß. Wir setzen

(120) $$a = da',\ m = dn,\ x = ghy.$$

Nach (118) muß $x^2 - a = g^2 h (hy^2 - a')$ durch $m = g^2 hn$ teilbar sein. Wir können daher (118) ersetzen durch

(121) $$hy^2 - a' = 0 \text{ nach dem Modul } n.$$

Haben h und n einen g. T., so müßte dieser nach (121) auch in a' aufgehen. Das aber ist nicht möglich, weil a' und n teilerfremd sind. Es hat daher (121) keine Lösung, wenn (h, n) nicht gleich 1 ist, und dann kann auch (118) keine haben. Es sei also $(h, n) = 1$. Dann ist nach dem Modul n die Zahl a'/h vorhanden und eindeutig bestimmt. Wir bezeichnen sie mit b. Da h zu n teilerfremd ist, so dürfen wir (121) durch h dividieren und erhalten so die mit (121) gleichwertige Gleichung

(122) $$y^2 - b = 0 \text{ nach dem Modul } n.$$

Es ist $(b, n) = 1$, so daß wir auf diese Gleichung die Ergebnisse der vorigen Nummer anwenden können. Sie hat also dann und nur dann Lösungen, wenn b QR von n ist. Diese Lösungen können wir nach der vorigen Nummer bestimmen und auch die Anzahl σ der nach n verschiedenen. Die σ Lösungen seien

(123) $$y_1, y_2, \ldots, y_\sigma.$$

Zu jeder dieser Lösungen dürfen wir Vielfache von n hinzufügen, so daß auch

(124) $$y_k, \; y_k \pm n, \; y_k \pm 2n, \ldots$$

Lösungen sind. Setzen wir $x_k = hgy_k$, so hat wegen (120) die Gleichung (118) die Lösungen

$$x_k = ghy_k, \; x_k \pm ghn, \; x_k \pm 2ghn, \ldots, \; (k = 1, 2, \ldots, \sigma).$$

Von diesen sind nach dem Modul $m = g \cdot ghn$ genau g verschieden, etwa

(125) $$x_k, \; x_k + ghn, \; x_k + 2ghn, \ldots, \; x_k + (g-1)ghn, \quad (k = 1, 2, \ldots, \sigma).$$

Hat also (118) überhaupt Lösungen, so ist die Anzahl der nach m verschiedenen gleich $g\sigma$. Ergebnis:

Die Gleichung

$$x^2 - a = 0 \quad \textit{nach dem Modul } m$$

hat dann und nur dann Lösungen, wenn folgende Bedingungen erfüllt sind: Es sei $(a, m) = g^2h$, *wo* h *nur Primzahlen in erster Potenz enthalten soll, und es sei* $a = g^2ha'$, $m = g^2hn$. *Dann muß erstens* $(h, n) = 1$ *sein, das heißt, es darf* m *keine in* a *in ungerader Potenz enthaltene Primzahl in einer höheren Potenz enthalten als* a. *Zweitens muß die dann nach dem Modul* n *vorhandene und eindeutig bestimmte Zahl* $b = a'/h$ *QR von* n *sein. Ist* σ *die Zahl der Werte von* $\sqrt{b}$ *nach dem Modul* n, *so ist* $g\sigma$ *die Zahl der Werte von* $\sqrt{a}$ *nach dem Modul* m.

17. Ein Beispiel.

Als Beispiel für die Lösung von (118) wählen wir

$$a = 153036 = 6^2 \cdot 13 \cdot 3 \cdot 109, \quad m = 180180 = 6^2 \cdot 13 \cdot 5 \cdot 7 \cdot 11.$$

Es ist

$$d = g^2h = 6^2 \cdot 13, \; g = 6, \; h = 13,$$
$$n = 5 \cdot 7 \cdot 11 = 385, \; a' = 3 \cdot 109 = 327.$$

Ferner wird

$$b = a'/h = 327/13 \quad \text{nach } 385 = 5 \cdot 7 \cdot 11.$$

Diese Gleichung zerfällt in die drei folgenden:

Nach 5: $b = 2/-2 = -1 = 4$;
Nach 7: $b = 327/-1 = -327 = 2$;
Nach 11: $b = -3/2 = 8/2 = 4$.

Die erste und dritte dieser Bedingungen sind erfüllt, wenn wir $b = 4 + 55u$ setzen und unter u irgendeine Zahl verstehen. Wir haben u so zu bestimmen, daß b nach 7 gleich 2 wird. Das gibt $55u = -2 = -u$ oder $u = 2$, so daß $b = 114$ wird.

Nach Nr. 16 haben wir jetzt die Lösungen von (122), also von

$$y^2 = 114 \quad \text{nach } 385 = 5 \cdot 7 \cdot 11$$

zu bestimmen. Zunächst suchen wir *eine* Lösung. Die anderen finden wir nach dem in Nr. 15 angegebenen Verfahren. Wir zerlegen die Gleichung für y in drei Gleichungen nach den Moduln 5, 7, 11. Nach 5: $y^2 = 4$, $y = 2$. Nach 7: $y^2 = 2 = 9$, $y = 3$. Nach 11: $y^2 = 4$, $y = 2$. Die erste und dritte Bedingung sind erfüllt, wenn wir $y = 2 + 55u$ setzen. Die ganze Zahl u haben wir so zu wählen, daß y nach 7 gleich 3 wird, also $55u$ gleich 1. Das ergibt $u = -1$ und $y = -53$. Da es auf das Vorzeichen nicht ankommt, so haben wir damit die beiden Lösungen ± 53. Um sämtliche Lösungen zu finden, zerlegen wir n auf alle möglichen Arten in zwei teilerfremde Faktoren. Das ergibt folgende acht Zerlegungen:

$$\begin{aligned} n = 385 &= 1 \cdot 385 = 385 \cdot 1, \\ &= 5 \cdot 77 = 77 \cdot 5, \\ &= 7 \cdot 55 = 55 \cdot 7, \\ &= 11 \cdot 35 = 35 \cdot 11. \end{aligned}$$

Die acht Werte von y erhalten wir dann durch die Bedingungen:

$$y_1 = \begin{cases} 53 & (385) \\ -53 & (1) \end{cases}, \qquad y_2 = \begin{cases} 53 & (1) \\ -53 & (385) \end{cases},$$

$$y_3 = \begin{cases} 53 & (77) \\ -53 & (5) \end{cases}, \qquad y_4 = \begin{cases} 53 & (5) \\ -53 & (77) \end{cases},$$

$$y_5 = \begin{cases} 53 & (55) \\ -53 & (7) \end{cases}, \qquad y_6 = \begin{cases} 53 & (7) \\ -53 & (55) \end{cases},$$

$$y_7 = \begin{cases} 53 & (35) \\ -53 & (11) \end{cases}, \qquad y_8 = \begin{cases} 53 & (11) \\ -53 & (35) \end{cases}.$$

Dabei bezeichnen die in Klammern gesetzten Zahlen die Moduln. Die Bedingungen für y_2, y_4, y_6, y_8 gehen aus denen für y_1, y_3, y_5, y_7 hervor durch Änderung des Vorzeichens der rechten Seite. Daher ist $y_2 = -y_1$, $y_4 = -y_3$, $y_6 = -y_5$, $y_8 = -y_7$. Zunächst ist selbstverständlich $y_1 = 53$, $y_2 = -53$. Wir können $y_3 = 53 + 77u$ setzen und erhalten die

Zahl u aus der Bedingung, daß y_3 nach dem Modul 5 gleich $-53 = -3$ sein muß. Das gibt $77u = 2u = -6$, $u = -3$ und $y_3 = 53 - 3 \cdot 77 = -178$, also $y_4 = +178$. In ähnlicher Weise findet man $y_5 = -y_6 = 108$, $y_7 = -y_8 = 123$. Aus jedem y_k erhalten wir eine Lösung x_k der gegebenen Gleichung, indem wir es mit $gh = 6 \cdot 13 = 78$ multiplizieren. Wir erhalten so acht Lösungen. Das sind aber nicht alle nach dem Modul m verschiedenen. Wir können noch zu jeder der Lösungen das Ein- bis $(g-1)$-fache, das heißt hier das Ein- bis Fünffache, von $ghn = 78 \cdot 385$ hinzufügen oder von ihr abziehen. Wir können auch so verfahren, daß wir zu jedem y_k die Zahl 385 fünfmal hinzufügen oder fünfmal von ihr abziehen. Wir wollen die Vielfachen von 385 zu den positiven y_k addieren und von den negativen subtrahieren. Wir erhalten so aus jedem y_k fünf neue Zahlen, im ganzen also $6 \cdot 8 = 48$ Zahlen, und zwar folgende:

± 53,	± 108,	± 123,	± 178,
± 438,	± 493,	± 508,	± 563,
± 823,	± 878,	± 893,	± 948,
± 1208,	± 1263,	± 1278,	± 1333,
± 1593,	± 1648,	± 1663,	± 1718,
± 1978,	± 2033,	± 2048,	± 2103.

Aus diesen Zahlen erhalten wir dann durch Multiplikation mit $gh = 78$ die Lösungen der gegebenen Gleichung. Ergebnis:

Die Gleichung

$$x^2 = 153036 \text{ nach dem Modul } 180180$$

hat folgende nach dem Modul verschiedene 48 Lösungen:

± 4134,	± 8424,	± 9594,	± 13884,
± 34164,	± 38454,	± 39624,	± 43914,
± 64194,	± 68484,	± 69654,	± 73944,
± 94224,	± 98514,	± 99684,	± 103974,
± 124254,	± 128544,	± 129714,	± 134004,
± 154284,	± 158574,	± 159744,	± 164034.

18. Eine Verallgemeinerung des Wilsonschen Satzes.

Es sei m eine positive Zahl, die größer als 2 sei. Wir setzen wieder $m = 2^\mu m_0$, wo m_0 ungerade sein soll. Es bedeute ferner wieder r die Anzahl der in m_0 enthaltenen verschiedenen Primzahlen. Zur Abkürzung sei $\varphi(m)$ mit s bezeichnet, und es seien $a_1, a_2, \ldots, a_s$ nach m verschiedene zu m teilerfremde Zahlen. Ihr Produkt sei g. Ist m eine Primzahl p, so ist g nach p gleich $(p-1)!$ und nach dem Wilsonschen Satze gleich -1. Wir wollen den Wert von g nach dem Modul m für beliebiges m zu be-

stimmen versuchen, und zwar auf dieselbe Art, wie wir den Wilsonschen Satz bewiesen haben. Wir teilen zunächst die a_k in zwei Gruppen. Die erste soll diejenigen a_k enthalten, die Lösungen der Gleichung $x^2 = 1$ nach m sind, die zweite alle anderen. Die Zahlen der ersten Gruppe seien mit $b_1, b_2, \ldots$, die der zweiten mit $c_1, c_2, \ldots$ bezeichnet. Da die Zahl 1 QR jeder Primzahl ist, und da 1 teilerfremd zu m ist, so hat die Gleichung $x^2 = 1$ nach m immer Lösungen, und diese sind teilerfremd zu m, so daß die b_i die sämtlichen nach m verschiedenen Lösungen sind. Ihre Anzahl ist nach Nr. 15 gleich 2^r, wenn $\mu = 0$ oder 1, gleich 2^{r+1}, wenn $\mu = 2$, und gleich 2^{r+2}, wenn $\mu \geqq 3$. Da wir den Fall $\mu = 1$, $r = 0$, nämlich $m = 2$, ausgeschlossen haben, so ist diese Zahl immer gerade. Sie sei mit 2τ bezeichnet. Da mit b_i auch immer $-b_i$ eine Lösung ist, und zwar eine von b_i verschiedene, so können wir die Bezeichnung so wählen, daß $b_2 = -b_1$, $b_4 = -b_3, \ldots, b_{2\tau} = -b_{2\tau-1}$. Es ist dann nach m

$$b_1 b_2 = -1, \quad b_2 b_3 = -1, \ldots, \quad b_{2\tau-1} b_{2\tau} = -1,$$

da ja $b_1^2 = b_3^2 = \cdots = b_{2\tau-1}^2 = 1$.

Wir betrachten jetzt die Zahlen c_i. Da sie teilerfremd zu m sind, so gibt es nach dem Modul m zu jeder Zahl c_k eindeutig die Zahl $1/c_k$, die mit c'_k bezeichnet sei. Es ist $c_k c'_k = 1$ nach m, so daß auch $c_k = 1/c'_k$. Die Zahl c'_k ist teilerfremd zu m; sie ist ferner von c_k verschieden, da sonst $c_k^2 = 1$ wäre und c_k zu den b_i gehören würde. Schließlich ist c'_k nicht eine der Zahlen b_i. Wäre etwa $c'_k = b_k$, so wäre $c'^2_k = 1$ und $c_k = 1/c'_k = c'_k = b_k$, was nicht sein kann. Es ist daher c'_k unter den c_i enthalten. Daraus ergibt sich, daß wir die c_i zu Paaren von je zwei verschiedenen so zusammenfassen können, daß das Produkt der beiden Zahlen eines Paares nach m gleich 1 ist. Bezeichnen wir die Anzahl der c_i mit 2ρ, so haben wir bei passender Numerierung der c_i die Gleichungen

$$c_1 c_2 = 1, \quad c_3 c_4 = 1, \ldots, \quad c_{2\rho-1} c_{2\rho} = 1.$$

Durch Multiplikation dieser Gleichungen und der oben für die b_i angegebenen erhalten wir

$$g = (-1)^\tau.$$

Dabei ist $\tau = 2^{r-1}$, wenn $\mu = 0$ oder 1, gleich 2^r, wenn $\mu = 2$, gleich 2^{r+1}, wenn $\mu \geqq 3$. Es ist also τ dann und nur dann ungerade, wenn

$$\mu = 0, \ r = 1 \ \text{oder} \ \mu = 1, \ r = 1 \ \text{oder} \ \mu = 2, \ r = 0.$$

Wir erhalten so folgende *Verallgemeinerung des Wilsonschen Satzes:*

Es sei m eine positive Zahl, und es sei g das Produkt von $\varphi(m)$ nach m verschiedenen, zu m teilerfremden Zahlen. Es ist dann nach dem Modul m die Zahl g gleich -1, wenn $m = 4$ oder gleich der Potenz einer ungeraden

Primzahl oder gleich dem doppelten einer solchen ist. In allen anderen Fällen ist g nach m gleich $+1$.

Wir hatten den Fall $m = 2$ ausgeschlossen. In diesem Falle ist $g = 1 = -1$.

VIII. Logarithmen.

1. Potenztabellen.

Wir rechnen nach einer ungeraden Primzahl p als Modul und stellen uns, wie in Abschnitt VI, Nr. 1, Tabellen her für die Potenzen der $p-1$ von 0 verschiedenen Zahlen

(126) $$1, 2, 3, \ldots, p-1.$$

Wir werden in diesem ganzen Abschnitt als Basen für Potenzen nur diese Zahlen (126) verwenden, also niemals die 0, was nicht jedesmal besonders hervorgehoben wird. Wie wir in Abschnitt VI gesehen haben, ist a^{p-1} für jedes von 0 verschiedene a gleich 1. Daraus folgt, daß sich eine Potenz a^{α} nicht ändert, wenn man sie ein oder mehrere Male mit a^{p-1} multipliziert oder dividiert, das heißt, wenn man zum Exponenten Vielfache von $p-1$ addiert oder von ihnen subtrahiert. Wir können uns daher bei den Exponenten auf die positiv kleinsten Reste

(127) $$0, 1, 2, \ldots, p-2$$

nach dem Modul $p-1$ beschränken. Wir haben uns zu merken: *Während wir bei den Potenzen nach dem Modul p rechnen, rechnen wir bei den Exponenten nach dem Modul $p-1$.* In der Potenztabelle (PT) für den Modul p brauchen wir daher nur die $p-1$ Zahlen (126) als Basen und die $p-1$ Zahlen (127) als Exponenten zu verwenden. Wir erhalten so quadratische Tabellen mit $p-1$ Zeilen und Spalten. Es folgen einige Beispiele. Es wird dem Leser empfohlen, sich weitere selbst herzustellen.

$p = 5$.

	0	1	2	3
1	1	1	1	1
2	1	2	4	3
3	1	3	4	2
4	1	4	1	4

$p = 7$.

	0	1	2	3	4	5
1	1	1	1	1	1	1
2	1	2	4	1	2	4
3	1	3	2	6	4	5
4	1	4	2	1	4	2
5	1	5	4	6	2	3
6	1	6	1	6	1	6

$p = 11.$

	0	1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6
3	1	3	9	5	4	1	3	9	5	4
4	1	4	5	9	3	1	4	5	9	3
5	1	5	3	4	9	1	5	3	4	9
6	1	6	3	7	9	10	5	8	4	2
7	1	7	5	2	3	10	4	6	9	8
8	1	8	9	6	4	10	3	2	5	7
9	1	9	4	3	5	1	9	4	3	5
10	1	10	1	10	1	10	1	10	1	10

$p = 13.$

	0	1	2	3	4	5	6	7	8	9	10	11
1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	3	6	12	11	9	5	10	7
3	1	3	9	1	3	9	1	3	9	1	3	9
4	1	4	3	12	9	10	1	4	3	12	9	10
5	1	5	12	8	1	5	12	8	1	5	12	8
6	1	6	10	8	9	2	12	7	3	5	4	11
7	1	7	10	5	9	11	12	6	3	8	4	2
8	1	8	12	5	1	8	12	5	1	8	12	5
9	1	9	3	1	9	3	1	9	3	1	9	3
10	1	10	9	12	3	4	1	10	9	12	3	4
11	1	11	4	5	3	7	12	2	9	8	10	6
12	1	12	1	12	1	12	1	12	1	12	1	12

2. Eigenschaften der PT.

Die PT für den Modul p haben in ihrem Bau sehr viel Ähnlichkeit mit den MT für den Modul $p-1$. Die Zeilen sind rein periodisch, und die Längen der Perioden sind Teiler von $p-1$. Die Zahlen einer Periode

sind voneinander verschieden. Das alles haben wir schon in Abschnitt VI bewiesen. Ferner bestehen die Perioden derselben Länge, abgesehen von der Reihenfolge, aus denselben Zahlen, und die Anzahl der Perioden der Länge l ist wieder $\varphi(l)$. Ist l' ein Teiler von l, so enthalten die Perioden der Länge l' nur Zahlen, die auch in denen der Länge l vorkommen. Wir wollen uns das Beispiel $p = 13$ genauer ansehen.

Zunächst stehen in der ersten Zeile und Spalte der PT lauter Einsen, während in der MT dort Nullen stehen. Es spielt ja die 1 bei der Multiplikation dieselbe Rolle wie die 0 bei der Addition. Die Potenzen von 2 bilden eine Periode der Länge $p - 1 = 12$. Wir können daher jede von 0 verschiedene Zahl als Potenz von 2 darstellen. So ist $3 = 2^4$. Wir können also die Potenzen von 3 der Reihe nach dadurch erhalten, daß wir, mit $3^0 = 1$ beginnend, immer mit 2^4, also viermal mit 2 multiplizieren, während wir die von 2 durch jedesmal einmaliges Multiplizieren mit 2 bekommen. Daraus folgt, daß wir die Potenzen von 3 der Reihe nach erhalten, indem wir die von 2 mit 4 auszählen. Da $11 = 2^7$, so erhalten wir die Potenzen von 11, indem wir die von 2 mit 7 auszählen. In dieser Weise können wir alle Zeilen der Tabelle aus Zeile 2 durch Auszählen erhalten. In derselben Weise konnten wir aber auch die Zeilen der MT für den Modul 12 aus Zeile 1 erhalten. Wir erhielten die Zeile a, das heißt die Vielfachen von a, durch Auszählen mit a. Hier erhalten wir die Zeile a, das heißt die Potenzen von a, durch Auszählen mit α, wenn $a = 2^\alpha$. Wollen wir daher in unserer PT dieselbe Anordnung der Zeilen haben, so müssen wir in die Zeile α die Potenzen von 2^α schreiben, so daß in den Zeilen der Reihe nach die Potenzen von

$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 3, \ldots, 2^{11} = 7$$

stehen. Bezeichnen wir die Zeilen der Reihe nach mit Zeile 0 bis Zeile 11, so erhalten wir jetzt sowohl bei der MT wie bei der PT Zeile α aus Zeile 1 durch Auszählen mit α. Die beiden Tabellen müssen daher jetzt in ihrem Bau vollkommen übereinstimmen. Die PT muß daher bei der neuen Anordnung der Zeilen auch die Symmetrieeigenschaften der MT haben. Es werden also auch ihre Spalten periodisch. Sie sei hier unter Fortlassung des linken und oberen Randes angegeben. (Siehe Tabelle Seite 88).

Da diese PT aus der Zeile 1, nämlich

(128) 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7

genau so entsteht wie die MT für den Modul 12 aus ihrer Zeile 1, nämlich

(129) 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,

so erhält man die PT aus der MT auch dadurch, daß man die Zahlen (129) der Reihe nach durch die Zahlen (128) ersetzt.

1	1	1	1	1	1	1	1	1	1	1	1
1	2	4	8	3	6	12	11	9	5	10	7
1	4	3	12	9	10	1	4	3	12	9	10
1	8	12	5	1	8	12	5	1	8	12	5
1	3	9	1	3	9	1	3	9	1	3	9
1	6	10	8	9	2	12	7	3	5	4	11
1	12	1	12	1	12	1	12	1	12	1	12
1	11	4	5	3	7	12	2	9	8	10	6
1	9	3	1	9	3	1	9	3	1	9	3
1	5	12	8	1	5	12	8	1	5	12	8
1	10	9	12	3	4	1	10	9	12	3	4
1	7	10	5	9	11	12	6	3	8	4	2

In derselben Art könnten wir allgemein schließen, daß die PT für den Modul p ihrem Bau nach mit der MT für den Modul $p-1$ übereinstimmt, wenn wir wüßten, daß in jeder PT eine Zeile vorkommt, die alle von 0 verschiedenen Zahlen enthält. Das aber ist nicht so einfach einzusehen.

3. Beweis der Eigenschaften der PT.

I. Eine Definition: Ist $a \neq 0$, *und ist* l *die kleinste positive Zahl, für die* $a^l = 1$, *so sagt man,* a *gehört zum Exponenten* l.

Wie wir schon in VI, 1 gesehen haben, gilt:

II. Gehört a *zum Exponenten* l, *so ist* a^α *dann und nur dann gleich 1, wenn* α *ein Vielfaches von* l *ist, und die Potenzen* $a^0, a^1, a^2, \ldots, a^{l-1}$ *sind voneinander verschieden.*

Es sei $b = a^\alpha$. Wir fragen uns, zu welchem Exponenten b gehört, wenn a zum Exponenten l gehört. Ist $b^m = a^{\alpha m} = 1$, so muß αm durch l teilbar sein. Ist $(\alpha, l) = d$, so ist das dann und nur dann der Fall, wenn m ein Vielfaches von l/d ist. Der kleinste positive Wert für m ist daher l/d, und es folgt:

III. Gehört a *zum Exponenten* l, *so gehört* a^α *zum Exponenten* $l/(\alpha, l)$. *Im besonderen gehört* a^α *dann und nur dann auch zum Exponenten* l, *wenn* $(\alpha, l) = 1$.

Ferner gilt:

IV. Gehören a *und* b *zu den Exponenten* l *und* m, *und ist* $(l, m) = 1$, *so gehört* ab *zum Exponenten* lm.

Ist nämlich $(ab)^n = a^n b^n = 1$, so folgt durch Potenzieren mit l und mit m

$$a^{ln} b^{ln} = (a^l)^n b^{ln} = b^{ln} = 1, \quad a^{mn} b^{mn} = a^{mn} (b^m)^n = a^{mn} = 1.$$

Es muß also ln durch m und mn durch l teilbar sein. Wegen $(l, m) = 1$ muß n Vielfaches von l und m, also auch von lm sein. Es ist daher, wie behauptet, lm der kleinste Wert von n, für den $a^n = 1$ ist.

Es mögen wieder a und b zu den Exponenten l und m gehören. Es sei l nicht durch m teilbar. Es enthält dann m mindestens eine Primzahl q in höherer Potenz als l. Es sei etwa

$$l = q^\lambda l', \quad m = q^\mu m', \quad \mu > \lambda, \text{ so daß } (l', q^\mu) = 1.$$

Setzen wir $a' = a^{q^\lambda}$, $b' = b^{m'}$, so gehören nach III. a' und b' zu den Exponenten l' und q^μ, und nach IV. gehört $a'b'$ zum Exponenten $l'q^\mu$, also zu einem größeren als a. Daraus schließen wir:

V. Ist n der größte von allen Exponenten, zu denen die Zahlen nach dem Modul p gehören, so ist n durch alle anderen Exponenten teilbar.

Gehörte nämlich etwa die Zahl b zu einem Exponenten m, der nicht in n aufgeht, so würden wir nach dem eben Bewiesenen eine Zahl finden können, die zu einem Exponenten gehört, der größer ist als n.

Es gehöre a zum Exponenten l, und es sei h ein positives Vielfaches von l. Dann ist

$$a^h - 1 = (a - 1)(1 + a + a^2 + \cdots + a^{h-1}) = 0.$$

Ist $a = 1$, so ist der erste Faktor 0, und der zweite hat den Wert h; ist aber $a \neq 1$, so muß der zweite Faktor verschwinden. Also:

VI. Setzen wir

$$s_h(x) = 1 + x + x^2 + \cdots + x^{h-1},$$

und ist h ein Vielfaches des Exponenten, zu dem a gehört, so ist

$$s_h(a) = \begin{cases} h, \text{ wenn } a = 1, \\ 0, \text{ wenn } a \neq 1. \end{cases}$$

Oder, anders ausgedrückt: Die Summe der Zahlen einer Periode, deren Länge größer ist als 1, ist immer 0 nach dem Modul p. Das kann man an den Tabellen leicht nachprüfen. Da die Potenzen $a^0, a^1, a^2, \ldots, a^{l-1}$ alle zu Exponenten gehören, die Teiler von l sind, und da nur a^0 gleich 1 ist, so ist im besonderen

$$(130) \quad s_l(a^\alpha) = 1 + a^\alpha + a^{2\alpha} + \cdots + a^{(l-1)\alpha} = \begin{cases} l \text{ für } \alpha = 0, \\ 0 \text{ für } \alpha = 1, 2, \ldots, l-1. \end{cases}$$

Eine der Eigenschaften der PT ist, daß die Zahlen einer Periode der Länge l' unter denen einer Periode der Länge l enthalten sind, wenn l' ein Teiler von l ist. Wir können das jetzt in folgender Form aussprechen:

VII. Gehören a und b zu den Exponenten l und m, und ist m ein Teiler von l, so ist b eine Potenz von a.

Um das zu beweisen, genügt es, zu zeigen, daß eine der Zahlen

(131) $$ba^0,\ ba^1,\ ba^2, \ldots,\ ba^{l-1}$$

gleich 1 sein muß. Ist etwa $ba^\beta = 1$, so wird ja $b = a^{-\beta} = a^{p-1-\beta}$. Durch den Satz VI haben wir die Möglichkeit gewonnen, die 1 von den anderen Zahlen zu unterscheiden. Die Zahlen (131) haben wegen der gemachten Voraussetzungen alle die Eigenschaft, daß ihre l-te Potenz gleich 1 ist. Wäre keine von ihnen gleich 1, so würde nach Satz VI für $h = l$,

(132) $$s_l(ba^\alpha) = 0 \text{ für } \alpha = 0, 1, 2, \ldots, l-1.$$

Es ist

$$\begin{aligned} s_l(ba^0) &= 1 + b + b^2 + \cdots + b^{l-1}, \\ s_l(ba^1) &= 1 + ba + b^2a^2 + \cdots + b^{l-1}a^{l-1}, \\ s_l(ba^2) &= 1 + ba^2 + b^2a^{2\cdot 2} + \cdots + b^{l-1}a^{(l-1)2}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ s_l(ba^{l-1}) &= 1 + ba^{l-1} + b^2a^{2(l-1)} + \cdots + b^{l-1}a^{(l-1)(l-1)}. \end{aligned}$$

Durch Addition folgt, wenn wir rechts immer die l untereinander stehenden Zahlen zusammenfassen,

$$s_l(ba^0) + s_l(ba^1) + \cdots + s_l(ba^{l-1}) = l + bs_l(a) + b^2s_l(a^2) + \cdots + b^{l-1}s_l(a^{l-1}).$$

Wegen (130) ergibt sich hieraus, daß die Summe der l Zahlen (132) gleich l ist, so daß sie nicht alle gleich 0 sein können. Daraus aber folgt, daß eine der Zahlen (131) (und nur eine) gleich 1 ist. Das aber war zu beweisen.

Es sei im besonderen g eine Zahl, die zu dem größten Exponenten n gehört. Da dann nach Satz V jede Zahl a zu einem in n enthaltenen Exponenten gehört, so ist nach dem eben bewiesenen Satze jede Zahl a eine Potenz von g. Es müssen daher unter den Potenzen von g alle $p-1$ von 0 verschiedenen Zahlen vorkommen. Das heißt die Periode der Potenzen von g muß die Länge $p-1$ haben, oder es gehört g zum Exponenten $p-1$. Wir haben daher:

VIII. Für jede ungerade Primzahl p gibt es mindestens eine Zahl g, die zum Exponenten p — 1 gehört.

IX. Eine Definition: Man nennt eine solche Zahl g eine primitive Kongruenzwurzel von p. Wir nennen sie eine Grundzahl für den Modul p.

Es sei noch ausdrücklich hervorgehoben, daß eine solche Grundzahl g die Eigenschaft hat, daß g^h dann und nur dann gleich 1 ist, wenn h durch $p-1$ teilbar ist. Mit Hilfe einer Grundzahl g können wir jetzt einmal die Zahlen bestimmen, die zu einem gegebenen Exponenten l gehören, deren Potenzen also Perioden der Länge l liefern, und dann diejenigen Zahlen, die in den Perioden der Länge l vorkommen. Es sei l ein Teiler

von $p-1$, und es sei $p-1 = dl$. Nach Satz III gehört die Zahl $a = g^\alpha$ — und in dieser Form läßt sich ja jede Zahl darstellen — zum Exponenten $(p-1)/(\alpha, p-1)$, also zum Exponenten l, wenn $(\alpha, p-1) = d$, wenn also $\alpha = dr$, wo r teilerfremd zu l ist. Da α eine der Zahlen von 0 bis $p-2$ ist, so ist r eine der Zahlen von 0 bis $l-1$. Daher ist die Anzahl der zum Exponenten l gehörenden Zahlen gleich der Anzahl derjenigen unter den Zahlen von 0 bis $l-1$, die zu l teilerfremd sind, also gleich $\varphi(l)$. Und wir haben:

X. *Es gibt $\varphi(l)$ Zahlen, die zum Exponenten l gehören, wenn l ein Teiler von $p-1$ ist. Im besonderen gibt es $\varphi(p-1)$ Grundzahlen für den Modul p.*

Die l in einer Periode der Länge l enthaltenen Zahlen seien

$$a_1, a_2, \ldots, a_l. \tag{133}$$

Diese Zahlen haben alle die Eigenschaft, daß ihre l-te Potenz gleich 1 ist. Ist wieder $p-1 = ld$, so ist die l-te Potenz von g^α dann und nur dann gleich 1, wenn αl durch $p-1$, wenn also α durch d teilbar ist. Es ist α eine der Zahlen von 0 bis $p-2$, und unter diesen gibt es genau l, die durch d teilbar sind, nämlich $0, d, 2d, \ldots, (l-1)d$. Daher sind die Zahlen (133), abgesehen von der Reihenfolge, identisch mit den Zahlen

$$g^0, g^d, g^{2d}, \ldots, g^{(l-1)d}.$$

Hieraus folgt auch wieder, daß die Perioden derselben Länge aus denselben Zahlen bestehen. Man vergleiche diese letzten Betrachtungen mit den entsprechenden bei den MT auf S. 21, 22.

4. Logarithmen.

Es sei g eine Grundzahl für die Primzahl p. Wir können dann jede der $p-1$ nach dem Modul p vorhandenen, von 0 verschiedenen Zahlen in der Form g^α darstellen. Dabei ist der Exponent bis auf Vielfache von $p-1$ eindeutig bestimmt. Rechnen wir also bei den Zahlen nach dem Modul p und bei den Exponenten nach dem Modul $p-1$, so gehört zu jeder von 0 verschiedenen Zahl ein Exponent und zu jedem Exponenten eine Zahl. Wir definieren:

Ist $a = g^\alpha$, so heißt α der Logarithmus von a, geschrieben

$$\alpha = \log a, \quad g^{\log a} = a.$$

Die Zahl g heißt die Basis der Logarithmen. Statt Logarithmus von a sagt man auch Index von a ($\operatorname{ind} a$). Die Zahl 0 hat keinen Logarithmus. Dabei ist bei den Zahlen nach dem Modul p und bei den Logarithmen nach dem Modul $p-1$ zu rechnen.

Wir geben für einige Primzahlen Logarithmentafeln, aus denen man zu jeder Zahl den Logarithmus und umgekehrt entnehmen kann.

p = *7. Basis 3.*

Zahl	1	2	3	4	5	6	nach 7
Log	0	2	1	4	5	3	nach 6

Log	0	1	2	3	4	5	nach 6
Zahl	1	3	2	6	4	5	nach 7

p = *11. Basis 2.*

Zahl	1	2	3	4	5	6	7	8	9	10	nach 11
Log	0	1	8	2	4	9	7	3	6	5	nach 10

Log	0	1	2	3	4	5	6	7	8	9	nach 10
Zahl	1	2	4	8	5	10	9	7	3	6	nach 11

p = *13. Basis 2.*

Zahl	1	2	3	4	5	6	7	8	9	10	11	12	nach 13
Log	0	1	4	2	9	5	11	3	8	10	7	6	nach 12

Log	0	1	2	3	4	5	6	7	8	9	10	11	nach 12
Zahl	1	2	4	8	3	6	12	11	9	5	10	7	nach 13

Die folgenden Tafeln schreiben wir mit zwei Eingängen, links die Zehner, oben die Einer.

p = *17. Basis 3.*

Logarithmen (nach 16).

	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

Zahlen (nach 17).

	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

p = *19. Basis 2.*

Logarithmen (nach 18).

	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

Zahlen (nach 19).

	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

$p = 23$. *Basis 5.*

Logarithmen (nach 22).

	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

Zahlen (nach 23).

	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

$p = 29$. *Basis 2.*

Logarithmen (nach 28).

	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

Zahlen (nach 29).

	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

$p = 31$. *Basis 3.*

Logarithmen (nach 30).

	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

Zahlen (nach 31).

	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Weitere Tabellen findet man im Canon arithmeticus von Jacobi.

Für $p = 31$ steht zum Beispiel $\log 25$ in der vorletzten Tabelle in Zeile 2 (Zehner von 25) und Spalte 5 (Einer von 25), so daß $\log 25 = 10$. Ebenso findet man $\log 17 = 7$. Umgekehrt findet man aus der letzten Tafel, daß zu den Logarithmen 13 und 27 die Zahlen 24 und 23 gehören. Auf eine Eigentümlichkeit der Tafeln für die Logarithmen sei noch hingewiesen. Die letzte Zahl ist immer $\frac{1}{2}(p-1)$. Woher kommt das? Diese letzte Zahl ist immer $\log(p-1)$. Die bemerkte Eigentümlichkeit sagt also aus, daß

$$\log(p-1) = \frac{1}{2}(p-1) = P,$$

wenn wir die schon früher öfter benutzte Abkürzung verwenden. Ist g die Basis der Logarithmen, so können wir statt dessen auch sagen: die P-te Potenz von g ist immer gleich $p-1=-1$. Wir haben in Abschnitt VI, Nr. 4 gesehen, daß die P-te Potenz jeder von 0 verschiedenen Zahl gleich $+1$ oder -1 ist. Da aber g eine Grundzahl für den Modul p ist, so ist erst die $(p-1)$-te Potenz von g gleich $+1$, und es muß die P-te Potenz gleich -1 sein. Zum Logarithmus P gehört also immer die Zahl $p-1=-1$.

5. Eigenschaften der Logarithmen.

Es sei $p=31$. Aus der Logarithmentafel ersehen wir, daß $19=3^4$, $26=3^5$, $28=3^{16}$. Daher wird

$$x = 19\cdot 26\cdot 28 = 3^{4+5+16} = 3^{25},$$

so daß $\log x = 25$ ist. Aus der Tafel für die Zahlen finden wir $x=6$. Wir ersehen daraus, daß durch Benutzung der Logarithmen eine Multiplikationsaufgabe in eine Additionsaufgabe verwandelt wird, und das ist die Hauptaufgabe der Logarithmen. Allgemein gilt Folgendes: Rechnen wir nach dem Modul p, wo p wieder eine ungerade Primzahl ist, und ist g die Basis der Logarithmen, so folgt aus

$$\log a = \alpha,\ \log b = \beta,\ \log c = \gamma,$$

oder, was dasselbe ist, aus

$$a = g^\alpha,\ b = g^\beta,\ c = g^\gamma:$$

$$a\cdot b = g^{\alpha+\beta},\ a\cdot b\cdot c = g^{\alpha+\beta+\gamma},\ a/b = g^{\alpha-\beta}$$

oder

$$(134)\qquad \begin{aligned} \log(ab) &= \alpha+\beta = \log a + \log b,\\ \log(abc) &= \alpha+\beta+\gamma = \log a + \log b + \log c,\\ \log(a/b) &= \alpha-\beta = \log a - \log b, \end{aligned}$$

woraus wir noch ersehen, daß Divisionsaufgaben auf Subtraktionsaufgaben zurückgeführt werden. Wählen wir $a=b=c$, so folgt

$$\log(a^2) = 2\log a,\ \log(a^3) = 3\log a$$

und allgemein für positives ganzzahliges n

$$(135)\qquad \log(a^n) = n\log a.$$

Aus der letzten der Gleichungen (134) folgt wegen $\log 1 = 0$

$$\log(1/a) = \log(a^{-1}) = \log 1 - \log a = -\log a.$$

Für positives ganzzahliges m wird in Verbindung mit (135)

$$\log(a^{-m}) = \log(a^{-1})^m = m\log(a^{-1}) = -m\log a.$$

Ist jetzt n eine negative Zahl, also $m = -n$ eine positive, so wird

$$\log(a^{-m}) = \log(a^n) = -m\log a = n\log a,$$

so daß (135) auch für negatives ganzzahliges n gilt. Schließlich gilt (135) auch für $n = 0$, wie man unmittelbar aus $\log 1 = 0$ folgert.

Aus (135) ersieht man, daß durch Logarithmieren das Potenzieren in Multiplizieren verwandelt wird. Damit hängt es zusammen, daß die PT für den Modul p so große Ähnlichkeit mit der MT für den Modul $p - 1$ hat. Man erhält diese aus jener, indem man ihre Zahlen durch deren Logarithmen ersetzt, bis auf die Anordnung der Zeilen. (Vgl. Nr. 2 dieses Abschnittes).

6. Anwendungen.

A. Multiplikations- und Divisionsaufgaben.

1. Zu berechnen $x = 7^3 \cdot 11^4 \cdot 5$ nach dem Modul 13. (Die Logarithmen sind nach dem Modul 12 zu nehmen).

$\log x = 3\log 7 + 4\log 11 + \log 5.$

$$\begin{array}{ll} \log 7 = 11 & \\ \log 11 = 7 & \\ \log 5 = 9 & \\ \mathbf{x = 10} & \end{array} \qquad \begin{array}{r} \left.\begin{array}{r} 3\log 7 = 33 = 9 \\ 4\log 11 = 28 = 4 \\ \log 5 = 9 = 9 \end{array}\right\} + \\ \hline \log x = 22 = 10 \end{array}$$

2. Zu berechnen

$$x = \frac{11^3 \cdot 8^5 \cdot 3^2}{13^2 \cdot 7^4 \cdot 5^6} = \frac{z}{n}$$

nach dem Modul 19. (Die Logarithmen sind nach dem Modul 18 zu nehmen).

$$\begin{aligned} \log x &= \log z - \log n, \\ \log z &= 3\log 11 + 5\log 8 + 2\log 3, \\ \log n &= 2\log 13 + 4\log 7 + 6\log 5. \end{aligned}$$

$$\begin{array}{l} \log 13 = 5 \\ \log 7 = 6 \\ \log 5 = 16 \end{array} \qquad \begin{array}{r} \left.\begin{array}{r} 2\log 13 = 10 = 10 \\ 4\log 7 = 24 = 6 \\ 6\log 5 = 96 = 6 \end{array}\right\} + \\ \hline \log n = 22 = 4 \end{array}$$

$$\begin{array}{l} \log 11 = 12 \\ \log 8 = 3 \\ \log 3 = 13 \\ \\ \mathbf{x = 2} \end{array} \qquad \begin{array}{r} \left.\begin{array}{r} 3\log 11 = 36 = 0 \\ 5\log 8 = 15 = 15 \\ 2\log 3 = 26 = 8 \end{array}\right\} + \\ \hline \left.\begin{array}{r} \log z = 23 = 5 \\ \log n = \quad 4 \end{array}\right\} - \\ \hline \log x = \quad 1 \end{array}$$

B. Diophantische Gleichungen. (Vgl. Abschnitt IV, Nr. 6).

1. Es sollen die ganzzahligen Lösungen der Gleichung

(136) $$19x - 23y = 5$$

bestimmt werden. Wie wir früher gesehen haben, genügt es, *eine* Lösung zu finden. Wir rechnen nach dem Modul 23, also bei den Logarithmen nach 22. Es wird

$$19x = 5,\ \log x = \log 5 - \log 19 = 1 - 15 = -14 = 8,$$

so daß sich $x = 16$ ergibt. Mit diesem Werte folgt aus (136)

$$23y = 19 \cdot 16 - 5 = 299 = 23 \cdot 13.$$

Es ist also

$$x = 16,\ y = 13$$

eine Lösung von (136). Die allgemeine ist dann nach IV, Nr. 6

$$x = 16 + 23u,\ y = 13 + 19u,$$

wo u irgendeine Zahl ist.

2. Es sollen die ganzzahligen Lösungen der Gleichung

(137) $$3689x - 2400y = 250$$

bestimmt werden.

Es ist $3689 = 7 \cdot 17 \cdot 31$. Nach dem Modul 7 ist $-2400y = -300y = -20y = y = 250 = 40 = 5$, also $\boldsymbol{y = 5}$ **nach 7.** Nach dem Modul 17 ist $-2400 = 14$, $250 = 12$, also $y = 12/14 = 6/7$.

$$\left.\begin{array}{l}\log 6 = 15\\ \log 7 = 11\end{array}\right\}-$$
$$\log y = 4, \quad \text{also } \boldsymbol{y = 13} \textbf{ nach 17.}$$

Nach dem Modul 31 ist $-2400 = 18$, $250 = 2$, also $y = 2/18 = 1/9$.

$$\left.\begin{array}{l}\log 1 = 0\\ \log 9 = 2\end{array}\right\}-$$
$$\log y = -2 = 28, \text{ also } \boldsymbol{y = 7} \textbf{ nach 31.}$$

Wir haben jetzt eine Zahl y zu bestimmen, die bei der Teilung durch 7, 17, 31 der Reihe nach die Reste 5, 13, 7 läßt (vgl. V, Nr. 6). Wir setzen

$$x_1 = 17 \cdot 31 y_1,\ x_2 = 7 \cdot 31 y_2,\ x_3 = 7 \cdot 17 y_3$$

oder $$x_1 = 527 y_1,\quad x_2 = 217 y_2,\quad x_3 = 119 y_3$$

und bestimmen y_1, y_2, y_3 so, daß

$$x_1 = 5 \text{ nach } 7,\ x_2 = 13 \text{ nach } 17,\ x_3 = 7 \text{ nach } 31.$$

Nach dem Modul 7:

$$x_1 = 527 y_1 = 2 y_1 = 5 = 12, \text{ so daß } \boldsymbol{y_1 = 6}.$$

Nach dem Modul 17:

$$x_2 = 217y_2 = 7 \cdot 31y_2 = 7 \cdot 14y_2 = 13,$$

$$\log y_2 = \log 13 - (\log 7 + \log 14) = 4 - (11 + 9) = -16 = 0,$$

so daß $\boldsymbol{y_2 = 1}$.

Nach dem Modul 31:

$$x_3 = 119y_3 = 7 \cdot 17y_3 = 7,\; 17y_3 = 1,$$

$$\log y_3 = -\log 17 = -7 = 23, \text{ so daß } \boldsymbol{y_3 = 11}.$$

Es wird daher

$$x_1 = 527 \cdot 6 = 3162,\; x_2 = 217,\; x_3 = 119 \cdot 11 = 1309$$

und

$$y = x_1 + x_2 + x_3 = 4688$$

oder, da wir y nach dem Modul $7 \cdot 17 \cdot 31 = 3689$ reduzieren dürfen,

$$y = 999.$$

Aus (137) folgt mit diesem Wert von y

$$3689\,x = 250 + 999 \cdot 2400 = 2\,397\,850 = 3689 \cdot 650,$$

so daß

$$x = 650,\; y = 999$$

eine Lösung der gegebenen Gleichung ist. Die allgemeine ist dann

$$\boldsymbol{x = 650 + 2400u,\quad y = 999 + 3689u,}$$

wo u irgendeine Zahl ist.

C. Ein Beweis des Wilsonschen Satzes.

In Nr. 5 des Abschnittes VII haben wir den Wilsonschen Satz bewiesen, der aussagt, daß dann und nur dann $(p-1)! = -1$ nach dem Modul p, wenn p eine Primzahl ist. Durch logarithmische Berechnung von $(p-1)!$ erhalten wir einen neuen Beweis. Es wird

$$\log\{(p-1)!\} = \log 1 + \log 2 + \log 3 + \cdots + \log(p-1),$$

so daß $\log\{(p-1)!\}$ gleich der Summe aller Logarithmen ist, die es zum Modul p gibt. Daher wird

$$\log\{(p-1)!\} = 0 + 1 + 2 + \cdots + (p-2)$$

$$= \frac{1}{2}(p-1)(p-2)$$

oder, da es auf Vielfache von $p-1$ nicht ankommt,

$$\log\{(p-1)!\} = \frac{1}{2}(p-1)\{(p-1)-1\} = -\frac{1}{2}(p-1) = +\frac{1}{2}(p-1).$$

Wie wir am Schluß von Nr. 4 dieses Abschnittes gesehen haben, gehört

zum Logarithmus $\frac{1}{2}(p-1)$ die Zahl -1. Daher ist nach dem Modul p, wie behauptet, $(p-1)! = -1$. Die Umkehrung kann so bewiesen werden wie an der früheren Stelle.

7. Wurzeln, Potenzreste.

Rechnen wir nach dem Modul p, so können wir mit der zugehörigen PT aus der Gleichung

$$a^n = b$$

eine Zahl bestimmen, wenn die beiden anderen gegeben sind. Das sind drei Arten von Aufgaben, je nachdem b, n oder a gesucht ist.

Die erste Aufgabe verlangt, die Zahl x aus der Gleichung

(138) $$x = a^n$$

zu bestimmen. Für $p = 13$ finden wir aus der Tabelle auf S. 86 z. B. $5^7 = 8$, $10^9 = 12$ usw.

Die zweite Aufgabe verlangt, die Zahl x aus der Gleichung

(139) $$a^x = b$$

zu bestimmen. Es wird also gefragt, ob sich eine Zahl b als Potenz einer anderen a darstellen läßt, und wenn ja, als welche. Für $p = 13$ haben wir z. B.: 3 läßt sich auf vier Arten als Potenz von 3 darstellen. Es ist $3 = 3^1 = 3^4 = 3^7 = 3^{10}$. Oder 4 läßt sich auf zwei Arten als Potenz von 10 schreiben, nämlich als 10^5 und 10^{11}. Dagegen läßt sich 2 weder als Potenz von 3 noch als Potenz von 10 darstellen. Die Gleichung (139) ist also nicht immer lösbar und, wenn sie es ist, nicht immer eindeutig. Nur wenn a eine der Grundzahlen für den Modul p ist, ist (139) immer, und zwar nur auf eine Art, zu lösen. Es ist ja dann x gleich dem Logarithmus von b zur Basis a.

Die dritte Aufgabe verlangt, die Zahl x aus der Gleichung

(140) $$x^n \quad b$$

zu bestimmen. Es wird also gefragt, ob sich eine Zahl b als n-te Potenz einer anderen darstellen läßt, oder ob sie nach dem Modul p gleich einer n-ten Potenz ist, oder ob es eine n-te Potenz gibt, die bei der Teilung durch p den Rest b läßt. Ist das der Fall, so heißt b ein n-ter Potenzrest. Man sagt nämlich:

Ist p eine Primzahl, und ist b eine nicht durch p teilbare Zahl, so heißt b ein n-ter Potenzrest von p, wenn es eine Zahl a gibt, deren n-te Potenz nach dem Modul p gleich b ist.

Für den Fall $n = 2$ ist uns diese Definition bekannt. Wir haben dann die quadratischen Reste.

Ist b ein n-ter Potenzrest von p, hat also die Gleichung (140) eine Lösung, so handelt es sich darum, alle Lösungen zu finden. Jede von ihnen heißt eine *n-te Wurzel* aus b (nach dem Modul p). Man schreibt

(141) $$x = \sqrt[n]{b}.$$

Es sei wieder $p = 13$. In der Tabelle auf S. 86 stehen in Spalte 5 die fünften Potenzen. Da in ihr alle $p - 1 = 12$ von 0 verschiedenen Zahlen, jede einmal, vorkommen, so ist $\sqrt[5]{a}$ für jedes a vorhanden und hat *einen* Wert. Zum Beispiel ist $\sqrt[5]{6} = 2$, $\sqrt[5]{10} = 4$ usw. In Spalte 9 stehen die neunten Potenzen. Wir sehen, in ihr kommen nur die Zahlen 1, 5, 8, 12 vor, und zwar jede dreimal. Diese und nur diese vier Zahlen sind daher neunte Potenzreste von 13, während 2, 3, 4, 6, 7, 9, 10, 11 es nicht sind. Wir finden aus der Tabelle für $\sqrt[9]{5}$ die drei Werte 2, 5, 6 und für $\sqrt[9]{1}$ die drei Werte 1, 3, 9. Die Zahlen in den Spalten der PT sind zur Abwechslung mal nicht periodisch. Wir haben aber an dem Beispiel $p = 13$ in Nr. 2 gesehen, daß wir sie durch passende Anordnung der Zeilen periodisch machen können (Vgl. die Tabelle auf S. 88). Wir gehen darauf nicht näher ein.

Der wesentliche Inhalt der PT findet sich in einfacherer und übersichtlicher Form in den Logarithmentafeln. Und wir können unsere drei Gleichungen (138), (139), (140) einfacher behandeln, indem wir zu den Logarithmen übergehen. So erhalten wir die drei Gleichungen

(142) $$\log x = n \log a, \quad x \log a = \log b, \quad n \log x = \log b,$$
$$\text{(nach dem Modul } p - 1).$$

Die erste Aufgabe gehört zu den in der vorigen Nummer unter A behandelten und ist ein besonders einfacher Fall. Die beiden anderen Aufgaben sind durch das Logarithmieren zu Divisionsaufgaben nach einer zusammengesetzten Zahl als Modul geworden. Wir können auf sie die Ergebnisse von Nr. 5 in Abschnitt IV anwenden (Vgl. den Satz über die Division auf S. 23). Wir beschränken uns auf die letzte Aufgabe. Übertragen wir den Satz auf S. 23 auf unseren Fall, so haben wir:

Es sei p eine ungerade Primzahl und n eine positive Zahl, die mit $p - 1$ den g. g. T. d habe. Es ist $\sqrt[n]{a}$ nach dem Modul p dann und nur dann vorhanden, wenn $\log a$ durch d teilbar ist. Die Anzahl der Werte von $\sqrt[n]{a}$ ist d.

Und auch:

Eine Zahl a ist dann und nur dann n-ter Potenzrest von einer ungeraden Primzahl p, wenn sie durch p nicht teilbar ist, und wenn $\log a$ durch $(n, p - 1)$ teilbar ist.

Beispiele:

1. $p = 19$.

$x^2 = 7$, $2 \log x = \log 7 = 6 = 24$, $\log x = 3$ oder 12, $x = \sqrt{7} = 8$ oder 11.

$x^2 = 8$, $2 \log x = \log 8 = 3$.

Da $\log 8$ gleich einer ungeraden Zahl ist, so können wir sie nicht durch 2 dividieren. Nun dürfen wir zwar zu $\log 8$ beliebige Vielfache von $p - 1 = 18$ hinzufügen, aber das nützt uns nichts, da $p - 1$ eine gerade Zahl ist, und die anderen Werte des Logarithmus daher auch ungerade sind. Nach dem Modul 19 ist daher $\sqrt{8}$ nicht vorhanden. Wir sehen daraus:

Eine durch p nicht teilbare Zahl ist QR oder QN von p, je nachdem ihr Logarithmus gerade oder ungerade ist.

$$x^5 = 9,\ 5 \log x = \log 9 = 8 \quad \text{nach } 18.$$

Da 5 zu 18 teilerfremd ist, so läßt sich nach dem Modul 18 jede Zahl durch 5 dividieren, und zwar eindeutig. Hier ist nach 18

$$\log x = 8/5 = -10/5 = -2 = 16,\ x = \sqrt[5]{9} = 5.$$

$$x^4 = 7,\ 4 \log x = \log 7 = 6 = 24 = 42 = 60 \text{ nach } 18.$$

Hier ist $(4,18) = 2$. Da $\log 7 = 6$ durch 2 teilbar ist, so kann man 6 durch 4 nach dem Modul 18 teilen, und man erhält die beiden Werte

$$\log x = 6/4 = 24/4 = 6 \text{ oder } \log x = 6/4 = 60/4 = 15,$$

woraus folgt

$$x = \sqrt[4]{7} = 7 \text{ oder } 12.$$

$$x^3 = 14,\ 3 \log x = \log 14 = 7 \quad \text{nach } 18.$$

Hier ist $(3,18) = 3$. Da $\log 14 = 7$ nicht durch 3 teilbar ist, so läßt sich nach dem Modul 18 die Zahl 7 nicht durch 3 teilen. Es ist daher $\sqrt[3]{14}$ nach dem Modul 19 nicht vorhanden.

2. $p = 31$.

$$x^{10} = 5,\ 10 \log x = \log 5 = 20 \quad \text{nach } 30.$$

Nach Nr. 8 in Abschnitt IV folgt hieraus

$$\log x = 2 \quad \text{nach } 3$$

oder

$$\log x = 2, 5, 8, 11, 14, 17, 20, 23, 26, 29 \quad \text{nach } 30,$$

$$x = \sqrt[10]{5} = 9, 26, 20, 13, 10, 22, 5, 11, 18, 21 \quad \text{nach } 31.$$

$x^{25} = 25,\ \ 25 \log x = \log 25 = 10$ nach 30,
$5 \log x = 2$ nach 6, $\log x = 2/5 = 20/5 = 4$ nach 6,
$\log x = 4, 10, 16, 22, 28$ nach 30,
$x = \sqrt[25]{25} = 19, 25, 28, 14, 7$ nach 31,
$x^9 = 6,\ \ 9 \log x = \log 6 = 25$ nach 30.

Hier ist $(9,30) = 3$ und $25 = \log 6$ ist nicht durch 3 teilbar. Daher ist $\sqrt[9]{6}$ nach dem Modul 31 nicht vorhanden.

8. Über die Verallgemeinerung des Logarithmus.

Es liegt nahe, eine Verallgemeinerung des Logarithmus auf den Fall zu versuchen, wo der Modul m eine zusammengesetzte Zahl ist. Es sei etwa g die Basis solcher Logarithmen. Hat g mit m den g. g. T d, so haben auch alle Potenzen von g mindestens den Teiler d mit m gemeinsam. Und, wenn g zu m teilerfremd ist, so sind es auch alle Potenzen von g. Man wird sich daher wie in dem Fall, wo m eine Primzahl p ist, auf die zu m teilerfremden Zahlen beschränken müssen und versuchen, diese als Potenzen einer passend gewählten Grundzahl g darzustellen. Da eine solche Zahl g zu m teilerfremd sein muß, so ist nach dem verallgemeinerten Fermatschen Satze

$$g^{\varphi(m)} = 1 \text{ nach } m.$$

Es sind daher von den Potenzen von g sicher höchstens $\varphi(m)$ verschieden. Es fragt sich, ob es wenigstens eine Zahl g gibt, deren erste $\varphi(m)$ Potenzen alle nach m voneinander verschieden sind. Eine solche Zahl könnten wir als Basis eines Logarithmensystems für die $\varphi(m)$ zu m teilerfremden Zahlen wählen. Eine derartige Zahl gibt es aber im allgemeinen nicht, wie schon einfache Beispiele zeigen. Für $m = 12$ ist $\varphi(m) = \varphi(12) = 4$, und die 4 zu 12 teilerfremden Zahlen sind 1, 5, 7, 11. Es ist schon die zweite Potenz dieser Zahlen nach 12 gleich 1, so daß es hier keine Zahl g der gewünschten Art gibt. Man sieht an diesem Beispiele außerdem, daß man nicht viel davon hätte, wenn es eine Zahl gäbe, deren vierte Potenz erst gleich 1 wäre. Denn auch dann könnte man nur für vier von den zwölf Zahlen, die es nach 12 gibt, einen Logarithmus definieren.

Eine genauere Betrachtung zeigt, daß man eine Zahl g, deren erste $\varphi(m)$ Potenzen nach m voneinander verschieden sind, dann und nur dann finden kann, wenn m die Potenz einer ungeraden Primzahl ist. Bezeichnen wir eine derartige Zahl mit *Grundzahl für den Modul m*, so gilt der *Satz:*

Ist m die Potenz einer ungeraden Primzahl p, so ist g eine Grundzahl für den Modul m dann und nur dann, wenn erstens g eine Grundzahl für den Modul p ist, und wenn zweitens $g^{p-1} - 1$ *zwar durch p, aber nicht*

durch p^2 teilbar ist. Ist ferner a eine Grundzahl für p, und ist $a^{p-1}-1$ durch p^2 teilbar, so ist $g=a+p$ eine Grundzahl für m.

Ehe wir diesen Satz beweisen, leiten wir zwei Formeln ab. Es seien b, c, n drei positive Zahlen. Dann ist nach dem Binomischen Satz

(143) $$(b+c)^n = b^n + n_1 b^{n-1} c + n_2 b^{n-2} c^2 + \cdots + c^n.$$

Hierin sind die Koeffizienten n_1, n_2 usw. ganze Zahlen. Im besonderen ist

(144) $$n_1 = n, \quad n_2 = \frac{1}{2}(n-1)n.$$

Ist $c=ap$ durch die ungerade Primzahl p teilbar, so folgt aus (143), (144)

(145) $$(b+ap)^n = b^n + napb^{n-1} \quad \text{nach } p^2.$$

Es sei jetzt $b=1$, $n=p$, und es sei $c=ap^\gamma$ durch p^γ teilbar, wo γ eine positive Zahl sein soll. Dann ist

$$n_2 c^2 = \frac{1}{2}(p-1)pp^{2\gamma}a^2$$

durch $p^{2\gamma+1}$ teilbar. Da $\gamma \geqq 1$, ist $2\gamma+1 \geqq \gamma+2$. Ferner sind die Potenzen c^3, c^4, ..., c^n alle mindestens durch $p^{\gamma+2}$ teilbar. Daher folgt aus (143), (144)

(146) $$(1+ap^\gamma)^p = 1 + ap^{\gamma+1} \quad \text{nach } p^{\gamma+2}.$$

Nunmehr gehen wir zum Beweis unseres Satzes über. Es sei g eine Grundzahl für den Modul p. Es ist $g^{p-1}=1$ nach p. Wir zeigen zunächst, daß wir annehmen können, daß $g^{p-1} \neq 1$ nach p^2. Es sei nämlich g_0 eine Grundzahl, für die $g_0^{p-1}=1$ nach p^2. Setzen wir $g=g_0+p$, so ist auch g eine Grundzahl, und es ist nach (145)

$$g^{p-1} = (g_0+p)^{p-1} = g_0^{p-1} + (p-1)pg^{p-2} \text{ nach } p^2.$$

Da nach Voraussetzung $g_0^{p-1}=1$ nach p^2, und da ferner $(g, p)=1$, so folgt

$$g^{p-1} = (g_0+p)^{p-1} = 1 + (p-1)pg^{p-2} \quad \text{nach } p^2.$$

Es ist daher $g^{p-1} \neq 1$ nach p^2. Wir setzen

(147) $$h_1 = g^{p-1} = 1 + a_1 p, \text{ wo } (a_1, p) = 1.$$

Es sei $\alpha \geqq 2$, und es sei l die kleinste positive Zahl, für die $g^l=1$ nach p^α. Dann sind die Zahlen

$$g^0, g^1, \ldots, g^{l-1}$$

nach p^α voneinander verschieden, und wenn $g^m=1$ nach p^α, so ist m durch l teilbar. Das folgt genau so, wie wir es bei Betrachtung der Potenzen für den Modul p (S. 37) bewiesen haben. Da g eine

Grundzahl ist, und da nach (147) $g^l = 1$ nach p, so muß l durch $p-1$ teilbar sein. Wir setzen

$$l = (p-1)\lambda.$$

Ferner ist nach dem verallgemeinerten Fermatschen Satz

$$g^{\varphi(p^\alpha)} = g^{p^{\alpha-1}(p-1)} = h_1^{p^{\alpha-1}} = 1 \quad \text{nach } p^\alpha. \tag{148}$$

Daher muß l ein Teiler von $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ sein. λ muß also eine Potenz von p sein. Es sei

$$\lambda = p^\beta.$$

Wegen (148) ist $\beta \leqq \alpha - 1$. Wir haben zu zeigen, daß das Gleichheitszeichen stehen muß.

Nach (147) ist

$$h_1 = 1 \quad \text{nach } p, \; h_1 \neq 1 \quad \text{nach } p^2.$$

Aus (146) folgt für $\gamma = 1$

$$h_1^p = 1 + a_1 p^2 \quad \text{nach } p^3.$$

Wir setzen

$$h_2 = h_1^p = 1 + a_2 p^2, \text{ wo } (a_2, p) = 1.$$

Es ist dann

$$h_2 = 1 \quad \text{nach } p^2, \; h_2 \neq 1 \quad \text{nach } p^3.$$

Aus (146) folgt für $\gamma = 2$

$$h_2^p = 1 + a_2 p^3 \quad \text{nach } p^4.$$

Wir setzen

$$h_3 = h_2^p = h_1^{p^2} = 1 + a_3 p^3, \text{ wo } (a_3, p) = 1.$$

Es ist also

$$h_1^{p^2} = 1 \quad \text{nach } p^3, \; h_1^{p^2} \neq 1 \quad \text{nach } p^4.$$

In dieser Weise können wir fortfahren und finden allgemein

$$h_1^{p^\beta} = 1 \quad \text{nach } p^{\beta+1}, \; h_1^{p^\beta} \neq 1 \quad \text{nach } p^{\beta+2}.$$

Es ist also im besonderen

$$h_1^{p^{\alpha-2}} \neq 1 \quad \text{nach } p^\alpha,$$

so daß $h_1^{p^\beta}$ erst für $\beta = \alpha - 1$ nach p^α gleich 1 wird.

Das war zu beweisen.

Wählen wir also g als Grundzahl, so können wir jede der $\varphi(p^\alpha)$ nach dem Modul p^α verschiedenen zu p teilerfremden Zahlen als Potenz von g darstellen. Ist etwa $a = g^\delta$, so setzen wir $\delta = \log a$. Wir haben also die Definitionsgleichung

$$g^{\log a} = a.$$

Mit den so definierten Logarithmen läßt sich genau so rechnen wie mit den früher für den Modul p definierten. Beispiele für Logarithmentafeln findet man im Canon arithmeticus von Jacobi (Berlin 1839).

Zum Schluß seien für ein weiteres Studium folgende Bücher empfohlen:

Bachmann, Paul: Zahlentheorie, I. Teil: Die Elemente der Zahlentheorie. Leipzig 1925.

Dickson-Bodewig: Einführung in die Zahlentheorie. Leipzig und Berlin 1931.

Hensel, Kurt: Zahlentheorie. Berlin und Leipzig 1913 bei Göschen.

Wertheim, Gustav: Anfangsgründe der Zahlenlehre. Braunschweig 1902.

Sachregister.

Absolut kleinste Reste 8
Additionstabelle 14f.

Basis eines Logarithmus 91

Diophantische Gleichungen 23, 96
Division nach einem Modul 19, 24, 25, 35

Echte Teiler 2
Elferprobe 13
Ergänzungssätze zum quadratischen Reziprozitätsgesetz 57
Eulersche φ-Funktion 26
Eulerscher Satz 56
Exponent, zu dem eine Zahl gehört 88

Fermatscher Satz 39f.
Fermatscher Satz, verallgemeinerter — 41, 44

Gaußscher Hilfssatz 60
Gemeinsamer Teiler 2, 3
Gemeinschaftliches Vielfaches 5
Größter gemeinsamer Teiler 2, 3
Grundzahl für einen Modul 90, 101

Index 91

Jacobi, Canon arithmeticus 93
Jacobisches Symbol 67

Kleinstes gemeinschaftliches Vielfaches 5
Kongruenzwurzel, primitive — 90

Legendresches Symbol 53, 64
Logarithmus 91ff., 101

Modul 10
Modul, Division nach einem — 19, 24, 25, 35
Modul, Grundzahl für einen — 101
Modul, Wurzel nach einem — 80, 99
Multiplikationstabelle 15ff.

Neunerprobe 13
Nichtrest, quadratischer — 50ff.
Nullteiler 22

Periode 20
Periodenlänge 20
Positiv kleinste Reste 8
Potenzrest 98
Potenztabelle 85ff.
Primitive Kongruenzwurzel 90
Primzahl 2, 6

Quadratischer Nichtrest 50ff.
Quadratischer Rest 49ff.
Quadratisches Reziprozitätsgesetz 59
Quadratisches Reziprozitätsgesetz, Ergänzungssätze zum — 57
Querdifferenz 13
Quersumme 12

Rest 1, 8
Rest, quadratischer — 49ff.
Reste, absolut kleinste — 8
Reste, positiv kleinste — 8
Restsystem, vollständiges oder volles — 8
Reziprozitätsgesetz, quadratisches 59

Teilbarkeitsregeln 11ff.
Teiler 1
Teiler, echter, eigentlicher — 2
Teiler, gemeinsamer — 2, 3
Teiler, größter, gemeinsamer — 2, 3
Teilerfremd 4

Vielfaches 1
Vielfaches, gemeinschaftliches — 5
Vielfaches, kleinstes, gemeinschaftliches — 5
Vollständiges oder volles Restsystem 8

Wilsonscher Satz 56, 83, 97
Wurzel nach einem Modul 80, 99

Zusammengesetzte Zahl 2

Elemente der Theorie der linearen Integralgleichungen.

Von Prof. **G. Vivanti.** Übersetzt und mit Anm. versehen von Fr. Schwank. 1929. XI und 296 Seiten Gr.-8°. Geb. 16.60 RM.

„**Frankfurter Zeitung**": Die moderne Theorie der linearen Integralgleichungen, eine Schöpfung der jüngeren Zeit, welche ihr Entstehen in erster Linie physikalischen Problemen verdankt, birgt für viele Untersuchungen solch erhebliche Vorteile in sich, daß auch der Ingenieur nicht achtlos an ihr vorbeigehen kann. Daher kann man es nur dankend anerkennen, daß Verfasser und Übersetzer dem deutschen, an diesen Dingen interessierten Publikum ein Werk vorlegen, das in hervorragendem Maße als eine gute Einführung in dieses Gebiet anzusehen ist.

Der Inhalt des Buches wird sicher am besten mit den Worten des Autors dahin gekennzeichnet, daß er die zum Studium der Originalarbeiten über Integralgleichungen notwendigen Hilfsmittel entwickelt. Die Darstellung bleibt auf die linearen Gleichungen beschränkt, enthält aber daneben Anwendungen auf die Theorie der linearen Differentialgleichungen und die theoretische Physik. Gerade im Interesse des Ingenieurs, der sich Kenntnisse auf diesem Gebiet wohl nur durch Privatstudium aneignen kann, sei anerkennend die gute pädagogische Darstellung der Materie hervorgehoben. Dieses Buch stellt zweifellos eine hervorragende Bereicherung der deutschen mathematischen Literatur dar und wird allen denen besonders willkommen sein, welche sich eingehende Kenntnisse auf diesem Gebiet aneignen wollen.

Dipl.-Ing. K. Schäfer.

„**Unterrichtsblätter für Mathematik und Naturwissenschaften**": Die sehr ausführlich gehaltene Darstellung wird allen denjenigen gute Dienste leisten, die sich ohne viel Vorkenntnisse mit den Methoden der Integralgleichungen vertraut machen wollen. Die zahlreich eingestreuten Beispiele tragen dazu bei, das Verständnis der allgemeinen Theorie zu vertiefen und damit die Anwendung auf konkrete Probleme zu erleichtern. Auch die Anmerkungen, die Fingerzeige für das erste Studium geben und für die wichtigsten Begriffe weitere Literatur nachweisen, werden dem Anfänger erleichtern, sich in dem Gebiete bald heimisch zu fühlen. Das ausführliche Verzeichnis der Lehrbücher und Abhandlungen, das in kurzen Stichworten den Inhalt kennzeichnet, wird für tiefere Studien von Nutzen sein. E. Salkowski.

Algebraische Flächen.

Von Prof. Dr. **Heinrich W. E. Jung.** XVI und 410 Seiten Gr.-8°. Geb. 21 RM.

„**Der Mittelschullehrer**": Dieses Werk ist eine sehr willkommene Erweiterung jener wundervollen algebraischen Theorie, die ihren Betrachtungen den Begriff des Körpers (Rationalitätsbereichs) zugrunde legt, deren Entdeckung und Ausbau mit den berühmtesten Namen der deutschen Geistesgeschichte der letzten Jahrzehnte verknüpft ist. —

Dieses interessante Werk verschafft dem aufmerksamen Leser hohen Genuß, setzt allerdings ziemlich umfangreiche Kenntnisse aus der Algebra, der Funktionstheorie, der Differentialgeometrie und der Invariantentheorie voraus und kostet selbst bei deren Vorhandensein stellenweise infolge der durchwegs abstrakten Darstellung mancherlei Mühe, die sich jedoch, wie stets beim Erarbeiten mathematischer Gedankengänge, sehr lohnt.

Mechanik.

Von Prof. Dipl.-Ing. **G. Haberland.** (Betriebstaschenbuch. Herausgegeben von Ministerialrat Prof. Dipl.-Ing. R. Horstmann und Prof. Dr.-Ing. K. Laudien.) (Bibl. der ges. Technik Bd. 322.) Zweite, neubearbeitete und erweiterte Auflage. 3.60 RM.

„**Werkstattechnik**", **Berlin**: Die Darstellung ist knapp und gedrängt, aber dabei von ausgezeichneter Klarheit. Ohne Verwendung höherer Mathematik, nur unter Voraussetzung einfachster geometrischer und algebraischer Vorkenntnisse, sind alle wichtigen Sätze abgeleitet, nicht allein die Resultate angegeben. Dadurch ist das Buch nicht bloß ein Nachschlage-, sondern ein Lehrbuch für mechanisches Verständnis geworden. Die graphische Darstellung steht gleichwertig neben der rechnerischen. Geschickt gewählte Beispiele aus der Praxis zeichnen den Anwendungsbereich der abgeleiteten Formeln. Das Büchlein kann aufs wärmste empfohlen werden.

Dr. S. Ledermann.

Verlagsverzeichnisse und Sonderprospekte kostenfrei.

Georg Dreyer

Statik und Festigkeit

I. Elemente der Graphostatik. Lehrbuch für höhere technische Lehranstalten und für den Selbstunterricht mit vielen Anwendungen auf den Maschinenbau, Eisenhoch- und Brückenbau. Zehnte Auflage. *5.90 RM.*

II. Festigkeitslehre und Elastizitätslehre. Lehrbuch für höhere technische Lehranstalten und für den Selbstunterricht. Zweite, neubearbeitete Auflage. 25×17,5 cm. 426 Seiten mit 452 Abbildungen. Geheftet 10.05 RM., gebunden 12.30 RM.

III. Erklärungen und Musterbeispiele zur Festigkeits- und Elastizitätslehre. Zweite Auflage. 7.55 RM.

IV. Formelsammlung zur Festigkeits- und Elastizitätslehre. Fünfte, vermehrte und verbesserte Auflage. 2.95 RM.

Die in zahlreichen Auflagen erschienene Graphostatik hat sich für den Unterricht sowohl wie auch für das Selbststudium als durchaus brauchbar erwiesen. Jeder Abschnitt ist durchsetzt mit zahlreichen, vollständig durchgeführten Musterbeispielen, die zum Teil so gewählt sind, daß ihre rechnerische Behandlung aus der Festigkeitslehre, Mechanik und dem Maschinenbau schon bekannt ist, so daß hier oft nur eine Wiederholung und Vertiefung des dort schon Gelernten durch die anschaulichere zeichnerische Darstellung geboten wird. Jeder Abschnitt enthält eine reichhaltige Sammlung von sorgsam geordneten Übungsaufgaben, die sich streng an die vorher besprochenen Beispiele anlehnen, deren Lösungen aber meistens nicht mitgeteilt sind, um den Studierenden zum selbständigen Nachdenken zu veranlassen. Über 320 sehr gut wiedergegebene Abbildungen und 5 Tafeln machen die Darstellung besonders anschaulich und leicht verständlich.

In dem Lehrbuch der Festigkeits- und Elastizitätslehre hat der Verfasser einen reichen Lehrstoff zugängig gemacht, der sowohl als Hilfsmittel für das Studium an höheren technischen Lehranstalten wie auch für den Selbstunterricht geeignet ist. Zahlreiche Beispiele und Übungsaufgaben sowie 413 klare, gut wiedergegebene Abbildungen erleichtern das Verständnis und vermitteln den Studierenden eine große Sicherheit auf dem hier vorgetragenen Gebiete.

Die Erklärungen und Musterbeispiele sind gleichzeitig die Antworten zu den Wiederholungsfragen und Lösungen zu den Übungsaufgaben in dem Lehrbuch der Festigkeits- und Elastizitätslehre des gleichen Verfassers, können aber auch unabhängig davon zur Belebung und Vertiefung des Studiums und zur Festigung des Gelernten verwendet werden. Sie werden dem Anfänger zu einer willkommenen Selbstprüfung und zu einer wertvollen Vertiefung seines Wissens dienen. Ein sorgfältiges Studium des Buches ist die beste Vorbereitung für die Prüfung. Alle Erklärungen sind so abgefaßt, daß sie auch ohne die Wiederholungsfragen des Lehrbuches eine zusammenhängende Übersicht über das ganze Gebiet geben. Da auch die Aufgaben selbst wiederholt sind, so bildet das Buch eine selbständige Sammlung von praktischen und theoretischen Aufgaben, die auch für den von Wert ist, der das Lehrbuch selbst nicht besitzt.

Bei der sorgfältig getroffenen Auswahl der Formelsammlung hat der Verfasser an erläuternden Abbildungen nicht gespart und bei ihrer Herstellung darauf geachtet, daß sie nicht nur die in den Formeln vorkommenden Buchstaben erklären, sondern auch Hinweise enthalten, durch die an die Herkunft der Formeln erinnert wird. Auf eine übersichtliche Anordnung und Zusammenfassung der Formeln für den praktischen Gebrauch ist besonders hingearbeitet.

Dr. Max Jänecke Verlagsbuchhandlung, Leipzig C 1